Model-Based Assurance Case+ (MBAC+): Tutorial on Modeling Radiation Hardness Assurance Activities

Rebekah Austin[1,2], Ken A. LaBel[2], Mike J. Sampson[2], John Evans[3], Art Witulski, Brian Sierawski[1], Gabor Karsai[1], Nag Mahadevan[1], Ron Schrimpf[1], Robert Reed[1]

1. Vanderbilt University; 2. NASA GSFC, 3. NASA HQ

This work is supported by NEPP and the NASA Reliability and Maintainability Program under Grant and Cooperative Agreement Number NNX16AR25G and NASA/JPL Subcontract Number 1568812

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.

Abbreviations and Acronyms

AMSAT: Radio Amateur Satellite Corporation

BN: Bayesian Network

COTS: Commercial Off-The-Shelf

ETW: Electronics Technology Workshop

GSN: Goal Structuring Notation

ITAR: International Traffic in Arms Regulations

JPL: Jet Propulsion Laboratory

MBAC+: Model-Based Assurance Case +

MBSE: Model-Based Systems Engineering

NASA: National Aeronautics and Space Administration

NEPP: NASA Electronic Parts and Packaging

R&M: Reliability & Maintainability

RHA: Radiation Hardness Assurance

SEAM: Systems Engineering and Assurance Models

SEFI: Single-Event Functional Interupt

SEL: Single-Event Latch-up

SEU: Single-Event Upset

SRAM: Static Random Access Memory

SysML: Systems Modeling Language

TID: Total Ionizing Dose

WDI: Watch-dog Input

WDO: Watch-dog Output

WDT: Watch-dog Timer

WebGME: Web-based Generic Modeling Environment

NASA/OSMA Electronic Parts and Packaging (NEPP) Program – Small Missions

Kenneth A. LaBel **Michael J. Sampson**

ken.label@nasa.gov **michael.j.sampson@nasa.gov**

301-286-9936 **301-614-6233**

Co- Managers, NEPP Program

NASA/GSFC

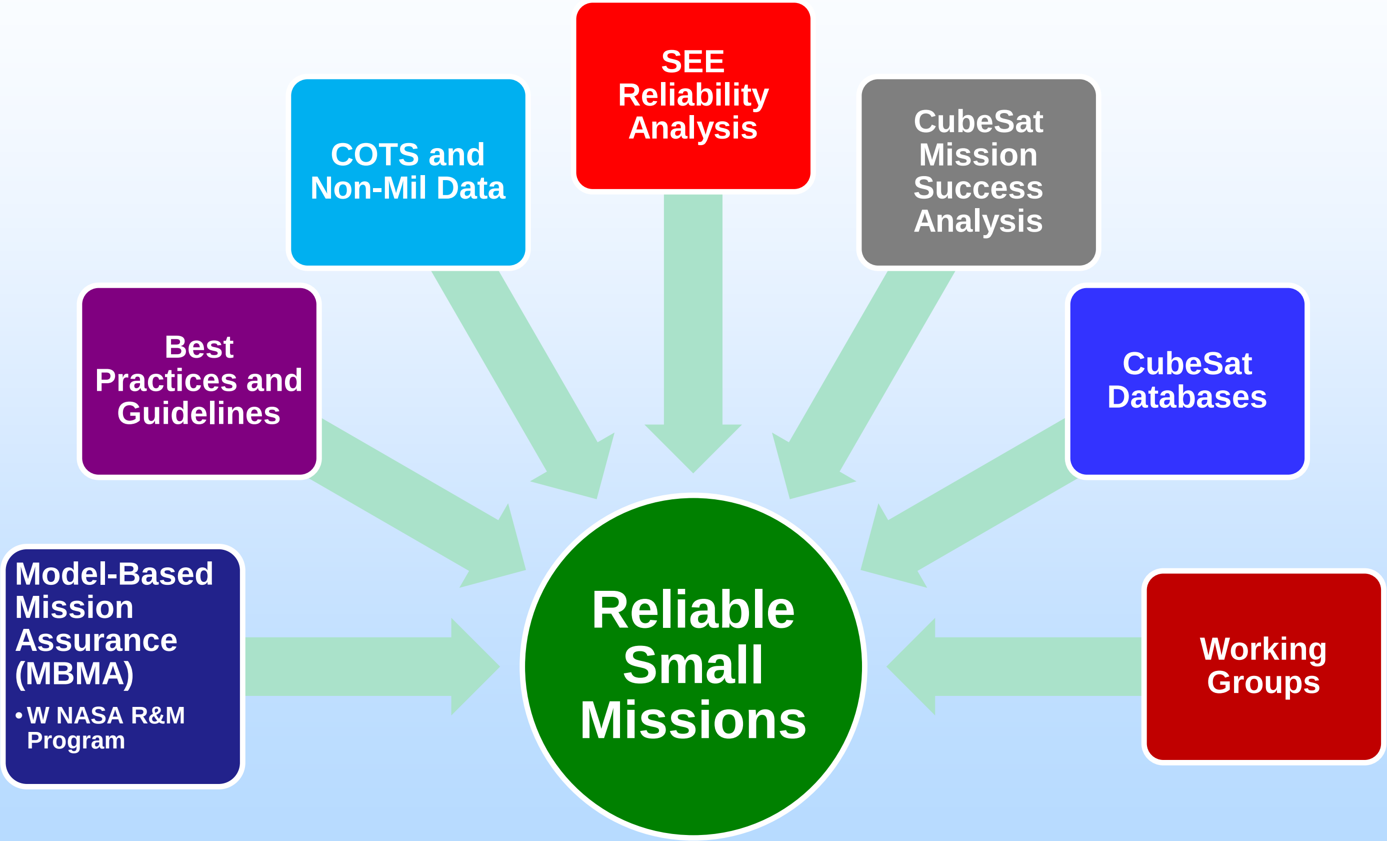
http://nepp.nasa.gov

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.

NEPP Small Mission History and Workshops

- FY13
  - Began discussions at https://nepp.nasa.gov/workshops/etw2013/talks.cfm
  - Held internal NASA meeting: EEE Parts for Class D Missions and CubeSats
    - Joint meeting supported by OSMA and OCE
- FY14
  - Discussion at annual workshop and (open) small mission workshop
    - https://nepp.nasa.gov/workshops/etw2014/talks.cfm
    - https://nepp.nasa.gov/workshops/eeesmallmissions/talks.cfm
    - NEPP plans updated based on feedback
- FY15
  - https://nepp.nasa.gov/workshops/etw2015/talks.cfm
- FY16
  - https://nepp.nasa.gov/workshops/etw2016/talks.cfm
- FY17 (talks to be posted in the next few weeks)
  - https://nepp.nasa.gov/workshops/etw2017/

NEPP - Small Mission Efforts



Reliable Small Missions

Model-Based Mission Assurance (MBMA)

- W NASA R&M Program

Best Practices and Guidelines

COTS and Non-Mil Data

SEE Reliability Analysis

CubeSat Mission Success Analysis

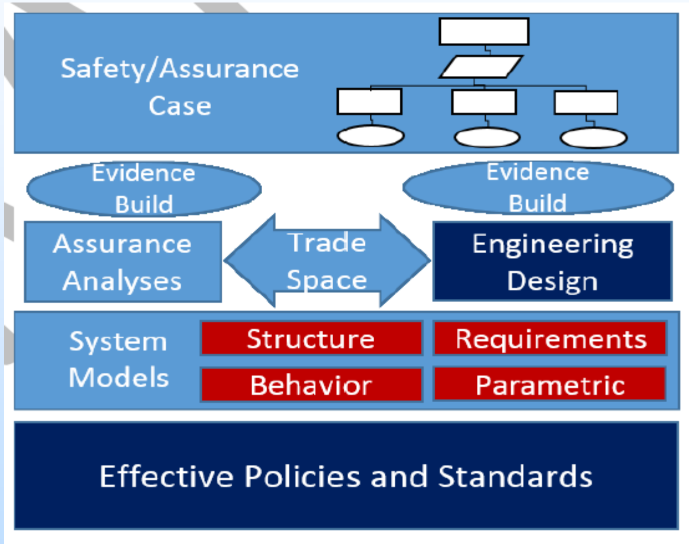
CubeSat Databases

Working Groups

FY18 task area ideas: automotive, avionics, and autonomous vehicles resilience

Model-Based Systems Engineering (MBSE) for Mission Assurance (MA) - aka MBMA

- Led by NASA/OSMA Reliability and Maintainability (R&M) Program
  - NEPP co-funds efforts that are EEE parts related (tasks listed below)
- Completed tasks (assurance case)
  - Vanderbilt University: Goal structuring notation (GSN) exemplar for single event effects (SEE) in a CubeSat electronics board
- Current tasks
  - Vanderbilt University:
    - Bayesian nets for CubeSat electronics (radiation)
    - On-line sysML/GSN tool for CubeSat electronics
      - TO BE DEMOED on July 18, 2017 at IEEE NSREC conference
- FY18 tasks (proposed)
  - Vanderbilt University:
    - Integrate Bayesian nets with on-line tool and complete assurance case
  - TBD:
    - Exemplar for EEE parts reliability (non-radiation)



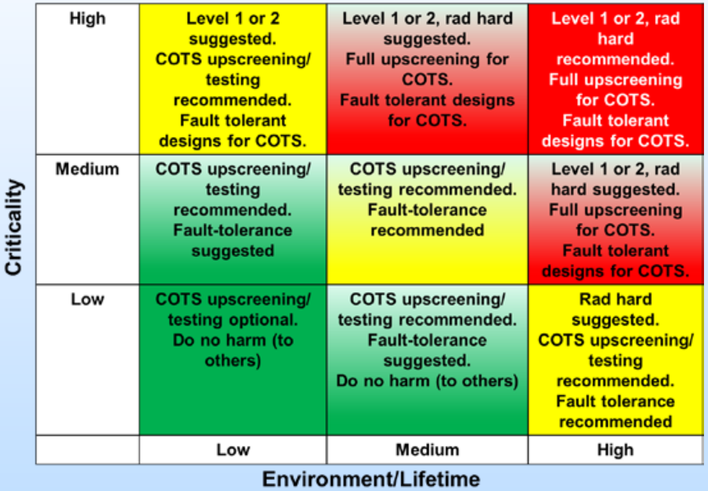
A Vision for Model Based Assurance

- John Evans, NASA/OSMA

Note: Mission Assurance Improvement Workshop (MAIW) is developing a MBSE for MA best practices document

Best Practices and Guidelines

- Current tasks
  - Radiation hardness assurance (RHA) for Small Missions
    - NASA/GSFC: Michael Campola
  - Board-level proton testing
    - JPL: Steve Guertin
  - Body of knowledge (BOK) on best practices for EEE part reliability via board testing
    - NASA/GSFC (Lentech): Ed Wyrwas
- Planned tasks
  - EEE Parts assurance for small missions
    - TBD (overdue)
  - Work with NASA/GSFC and NASA STMD for release of CubeSat tool
    - R-GENTIC (Michael Campola)
      - R – Radiation GuidelinEs for Notional Threat Identification and Classification
    - *Plan is to make available via the web (NEPP website) and demo at IEEE NSREC*



Criticality			
High	Level 1 or 2 suggested. COTS upscreening/ testing recommended. Fault tolerant designs for COTS.	Level 1 or 2, rad hard suggested. Full upscreening for COTS. Fault tolerant designs for COTS.	Level 1 or 2, rad hard recommended. Full upscreening for COTS. Fault tolerant designs for COTS.
Medium	COTS upscreening/ testing recommended. Fault-tolerance suggested	COTS upscreening/ testing recommended. Fault-tolerance recommended	Level 1 or 2, rad hard suggested. Full upscreening for COTS. Fault tolerant designs for COTS.
Low	COTS upscreening/ testing optional. Do no harm (to others)	COTS upscreening/ testing recommended. Fault-tolerance suggested. Do no harm (to others)	Rad hard suggested. COTS upscreening/ testing recommended. Fault tolerance recommended
	Low	Medium	High

Environment/Lifetime

NEPP Notional EEE Parts Assurance - Tailored Risk Acceptance

Note: MAIW is developing a CubeSat Best Practices for Mission Success (Test) document

Non-Mil/Aero EEE Parts

- Automotive grade
  - Began FY15
    - Snapshot of representative part types under evaluation for reliability
  - Began FY16
    - Support of NASA Engineering Safety Center (NESC) automotive grade tests (limited electrical tests and a few radiation tests)
  - Plans
    - Guideline/lessons learned
    - Resilience/soft error rate – challenge in finding a partner
    - Have begun partnership with The Aerospace Corp
- COTS
  - Testing of COTS has been a cornerstone of the NEPP Program including processors, memories, FPGAs, power devices, etc…
    - Multiple on "CubeSat" class electronics - see presentations at weblinks on chart 2.
      - Example: radiation data on TI MSP430 processors
  - Plans
    - Discuss FY18 tasks for "CubeSat" class EEE parts
    - Plastic encapsulated device guideline
- NEPP radiation data can found at
  - http;//nepp.nasa.gov
  - http://radhome.gsfc.nasa.gov
  - Or via IEEE search

NEPP CubeSat Success and Databases

- Mission Success Analysis (Prof. Michael Swartwout/SLU)
  - NEPP has been funding on-going tracking of CubeSat mission success with newer emphasis on root-cause (improved assurance practices)
    - Note: Prof. Swartwout is teaching a short course session on this topic at IEEE NSREC on July 17, 2017
- CubeSat Databases
  - JPL: two studies (need to update studies or tie into other studies)
    - Kit manufacturer EEE parts approaches
    - What EEE parts NASA (and JPL) are using in CubeSats
  - JPL: Limited evaluation of CubeSat kit electronics boards
  - JPL Action: integrate databases with The Aerospace Corp, SPOON database and with success study (if possible)
    - New: discuss with Ames (Small Spacecraft Virtual Institute)

Radiation Reliability Analysis and Working Group

- Single event effect (SEE) reliability analysis
  - NASA/GSFC (Melanie Berg/AS&D) - Current effort focused on developing model for treating SEE in a manner similar to reliability (i.e., how many 9's rather than a SEE rate)
  - Planned task is integration with MBMA tools approach
- Working groups
  - NEPP working group meets monthly on "CubeSat databases"
    - The Aerospace Corp and Prof. Swartwout participate
  - Support of MAIW (by invitation meetings with public document release)
  - Support of The Small Satellite Reliability Initiative- A Public-Private Collaboration (POC: Mike Johnson – NASA/GSFC)

“A Working List of Priorities"

- **Key thought: What do we need to do to enable “higher reliability” small (cost-effective) missions?**
  - **NEPP website is expected to go through a major overhaul in the next few months**
    - **Improved access to “bigger thoughts” (guidelines, best practices)**
    - **COTS data, and so on**
  - **Improve “COTS” data sharing**
  - **Extend COTS testing**
  - **Extend model-based mission assurance**
    - **Guidance on “tailoring” of approaches**
  - **Best practices are OVERDUE for EEE parts**
  - **What can we learn (or jointly learn) from resilience approaches?**

Model-Based Assurance Case+ (MBAC+): Tutorial on Modeling Radiation Hardness Assurance Activities

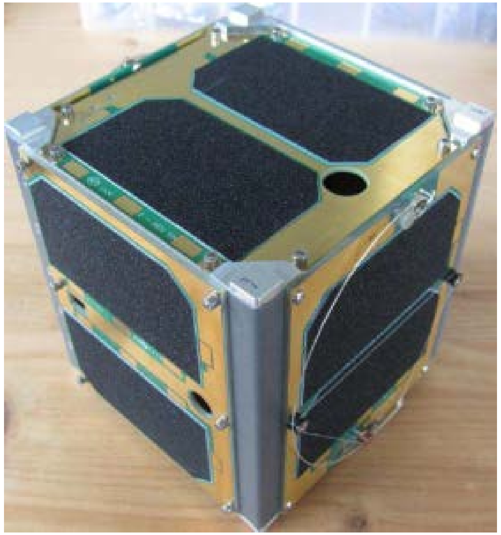
Rebekah Austin

This work is supported by NEPP and the NASA Reliability and Maintainability Program under Grant and Cooperative Agreement Number NNX16AR25G and NASA/JPL Subcontract Number 1568812

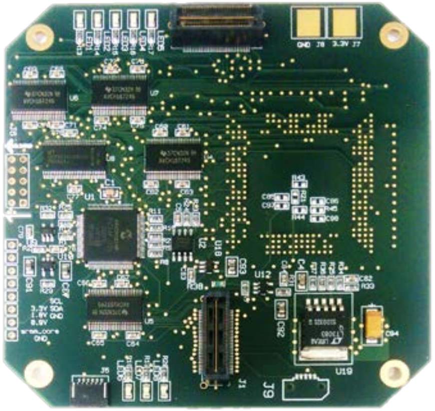
To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.

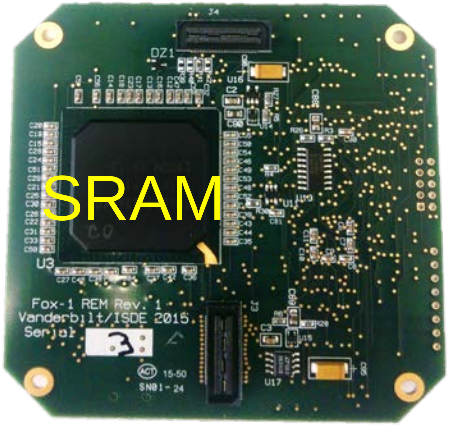
Radiation Reliability Assessment of CubeSat SRAM Experiment Board

- **Assessment completed on 28nm SRAM SEU experiment**
- **Reasons for integrated modeling**
  - Use commercial off-the-shelf (COTS) parts
  - System mitigation of SEL
  - High risk acceptance



Courtesy of AMSAT

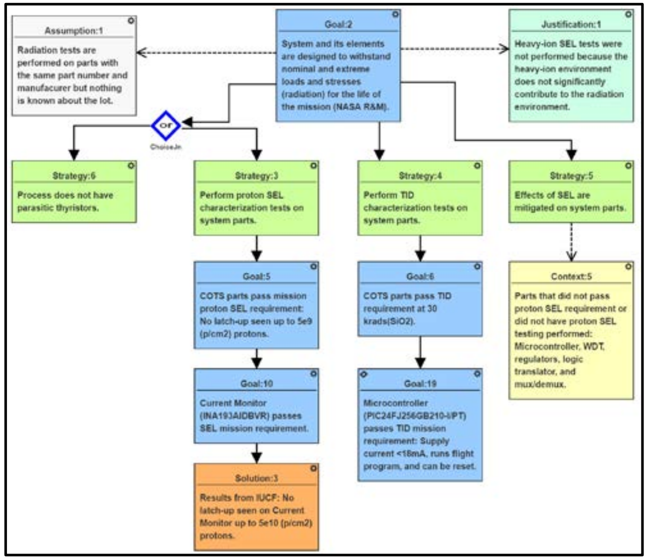




At the end of this tutorial you will:

- Understand the reasons for modeling a radiation hardness assurance case for a system
- Understand the basics of graphical argument representation and system modeling with block diagrams and fault propagation
- Have seen a simple example for single-event latch-up (SEL) mitigation on commercial off-the-shelf (COTS) parts
- Know the basics about using modelbasedassurance.org to model assurance cases for radiation reliability

MBAC+ Modeling Flow



Assumption:1

Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:2

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1

Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6

Process does not have parasitic thyristors.

Strategy:3

Perform proton SEL characterization tests on system parts.

Strategy:4

Perform TID characterization tests on system parts.

Strategy:5

Effects of SEL are mitigated on system parts.

Goal:5

COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6

COTS parts pass TID requirement at 30 krads(SiO2).

Context:5

Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10

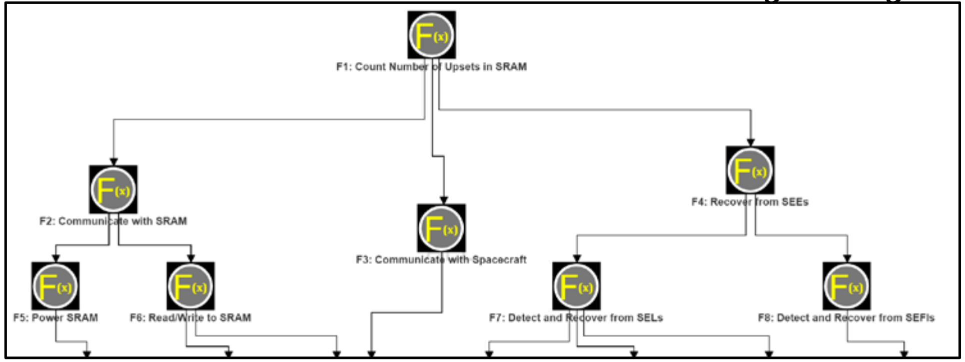
Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19

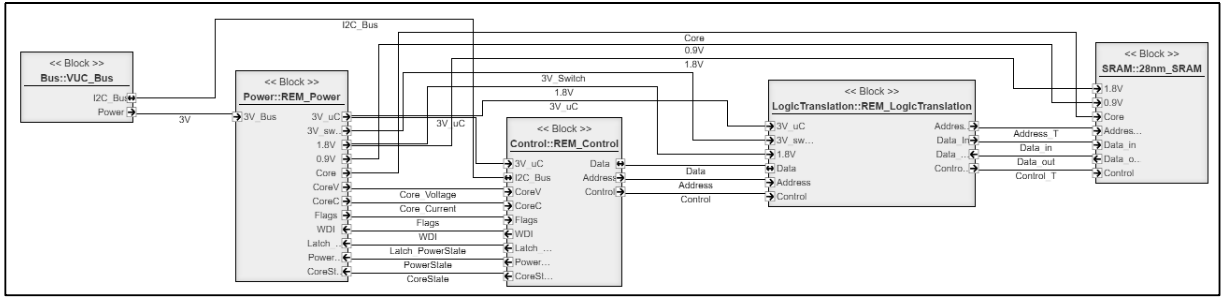
Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3

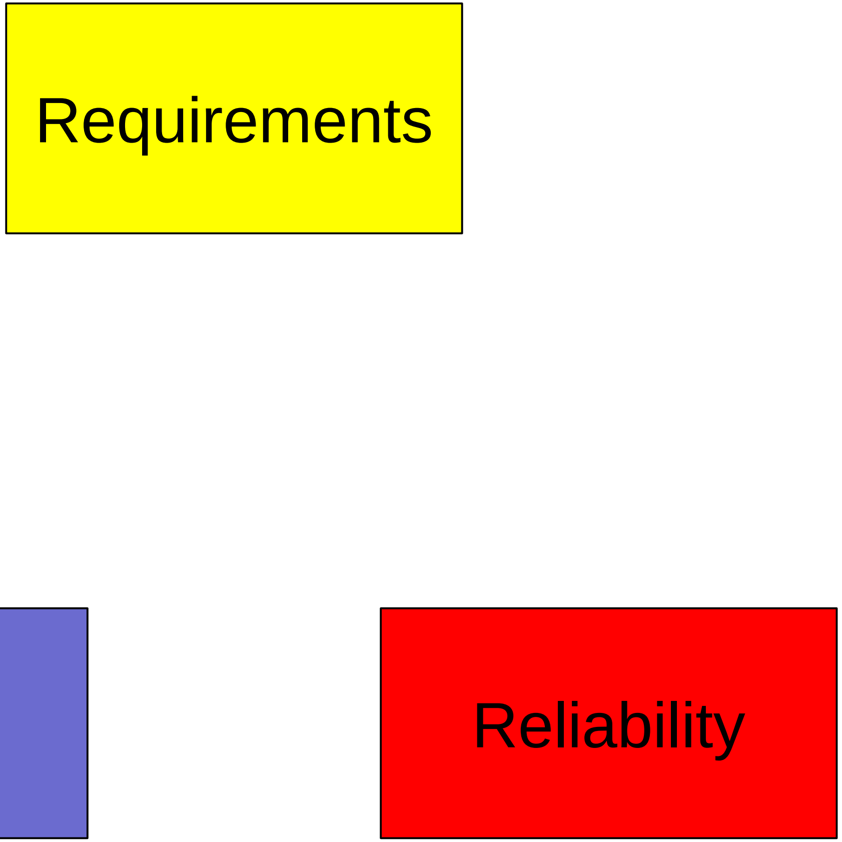
Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.



F(x)
F1: Count Number of Upsets in SRAM
F2: Communicate with SRAM
F3: Communicate with Spacecraft
F4: Recover from SEEs
F5: Power SRAM
F6: Read/Write to SRAM
F7: Detect and Recover from SELs
F8: Detect and Recover from SEFIs



Integrated System Design for Radiation Environments

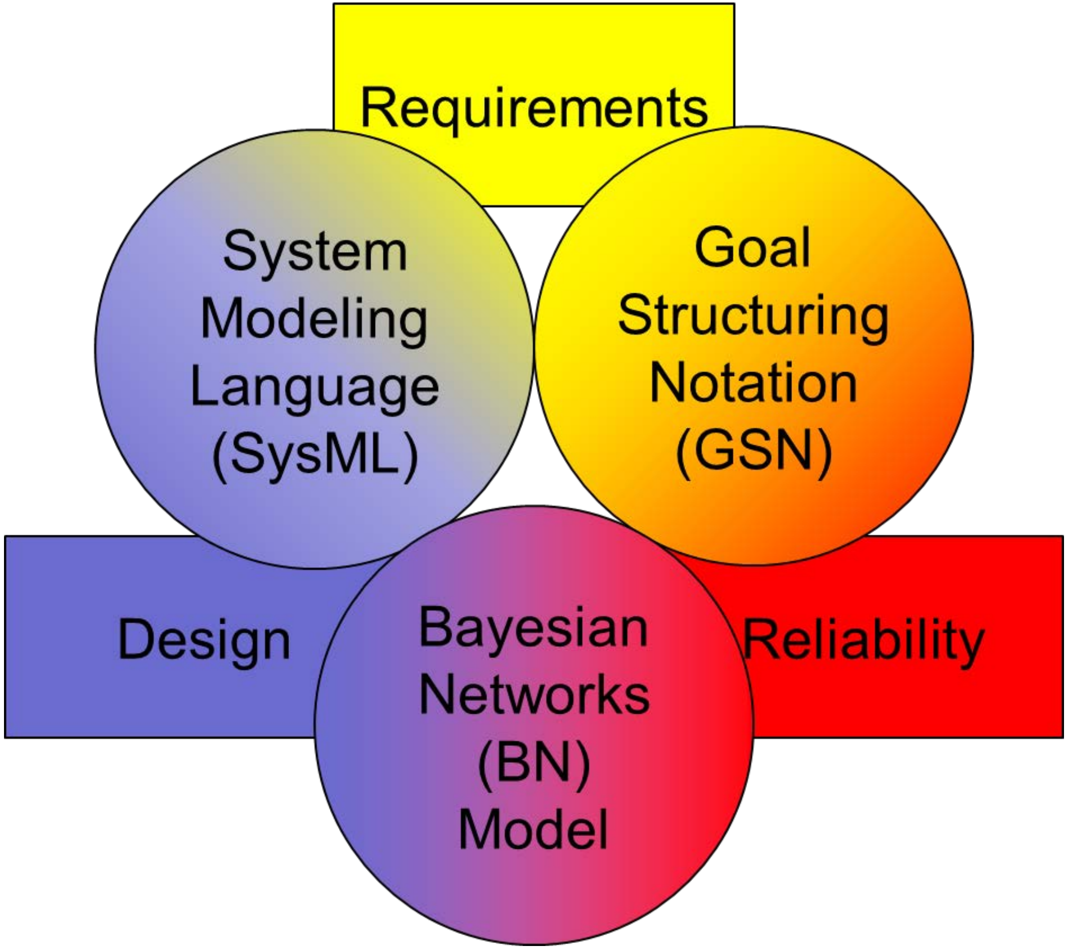


Requirements

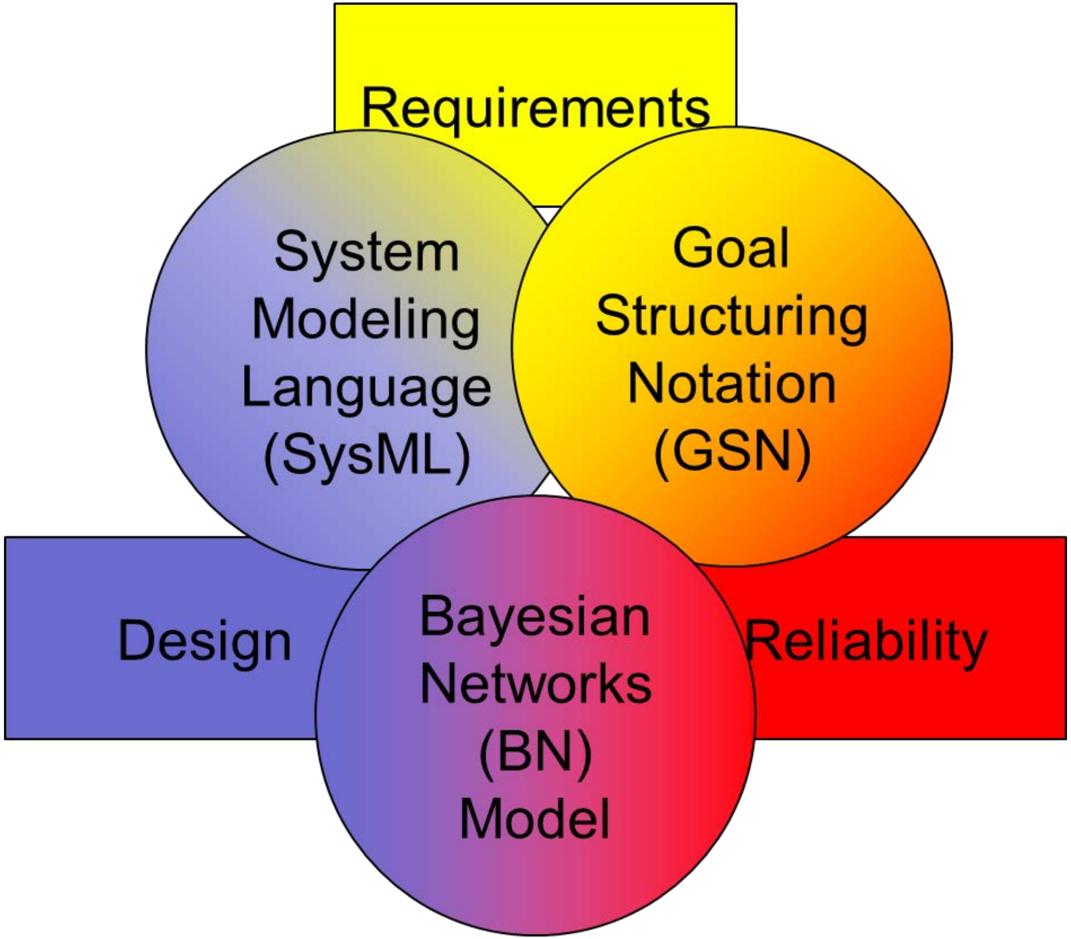
Design

Reliability

Integrated System Design for Radiation Environments

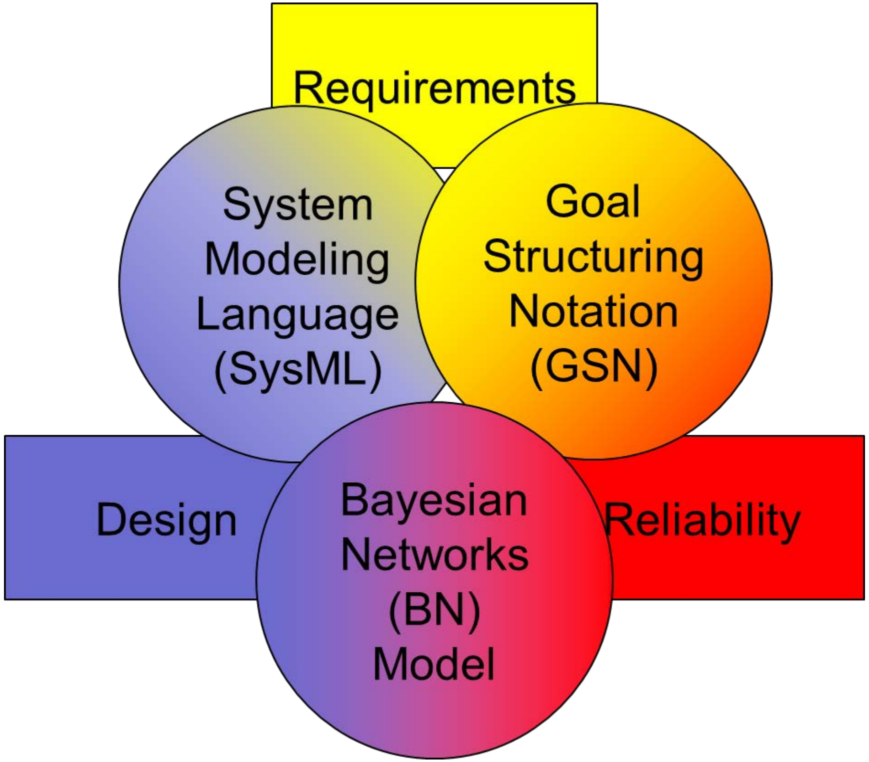

Requirements
System Modeling Language (SysML)
Goal Structuring Notation (GSN)
Design
Bayesian Networks (BN) Model
Reliability

Integrated System Design for Radiation Environments


Requirements
System Modeling Language (SysML)
Goal Structuring Notation (GSN)
Design
Bayesian Networks (BN) Model
Reliability

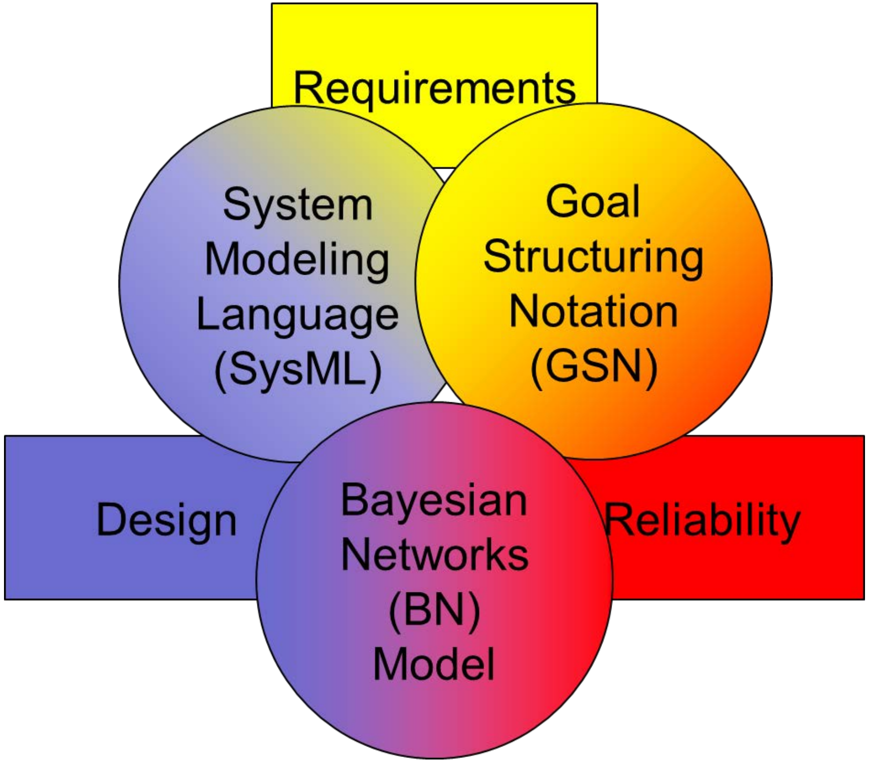
Integrated System Design for Radiation Environments

- **Reasons for Activity interaction**
  - Commercial parts (COTS)
  - Document-centric work flow to model-based system engineering
  - System mitigation (for COTS)
  - Shorter schedules for small spacecraft


Requirements
System Modeling Language (SysML)
Goal Structuring Notation (GSN)
Design
Bayesian Networks (BN) Model
Reliability

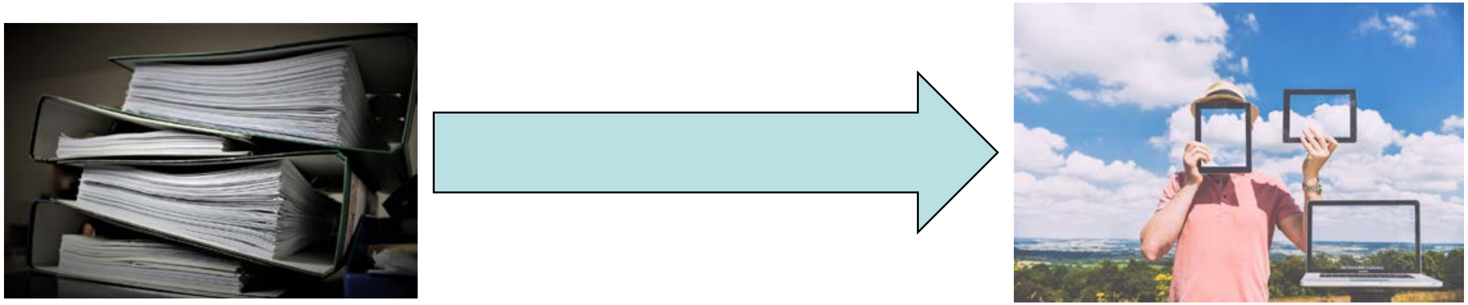
Model-Based Assurance Case + (MBAC+)

- **Goal Structuring Notation:**
  - R&M Template
  - Visual representation of argument
- **System Modeling Language (SysML):**
  - Specification of systems through standard notation
- **Bayesian Network (BN)**
  - Nodes describe probabilities of states
  - Calculate conditional probabilities from observations


Requirements
System Modeling Language (SysML)
Goal Structuring Notation (GSN)
Design
Bayesian Networks (BN) Model
Reliability

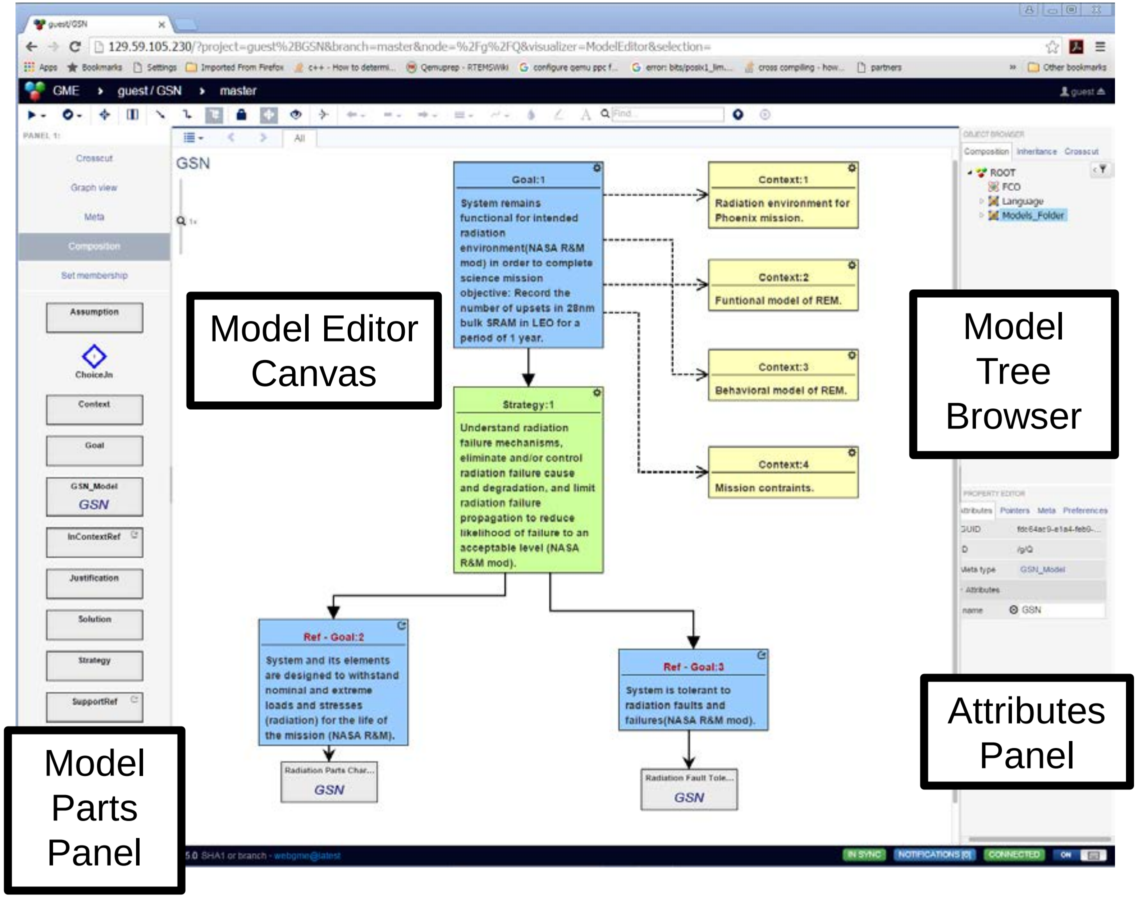
What is System Engineering and Assurance Models (SEAM)?

- **A set of modeling languages in one environment used to implement MBAC+**
- **These modeling languages allow for reliability activities and requirements to become part of the Model-Based System Engineering (MBSE) paradigm**
  - Move from document-based reliability to objective-based reliability
  - Takes Radiation Hardness Assurance activities from being a process that results in ***unlinked and unrelated*** documents and integrates those activities into the overall system design process



What is SEAM? Cont.

- **SEAM is built using WebGME tool**
- **Models include:**
  - Goal Structuring Notation (GSN)
  - System model (SysML)
  - Fault Propagation
  - Function/Behavior Models
- **Allows for links across models**
- **Links to external documents**



Goal:1
System remains functional for intended radiation environment(NASA R&M mod) in order to complete science mission objective: Record the number of upsets in 28nm bulk SRAM in LEO for a period of 1 year.

Context:1
Radiation environment for Phoenix mission.

Context:2
Funtional model of REM.

Context:3
Behavioral model of REM.

Context:4
Mission contraints.

Strategy:1
Understand radiation failure mechanisms, eliminate and/or control radiation failure cause and degradation, and limit radiation failure propagation to reduce likelihood of failure to an acceptable level (NASA R&M mod).

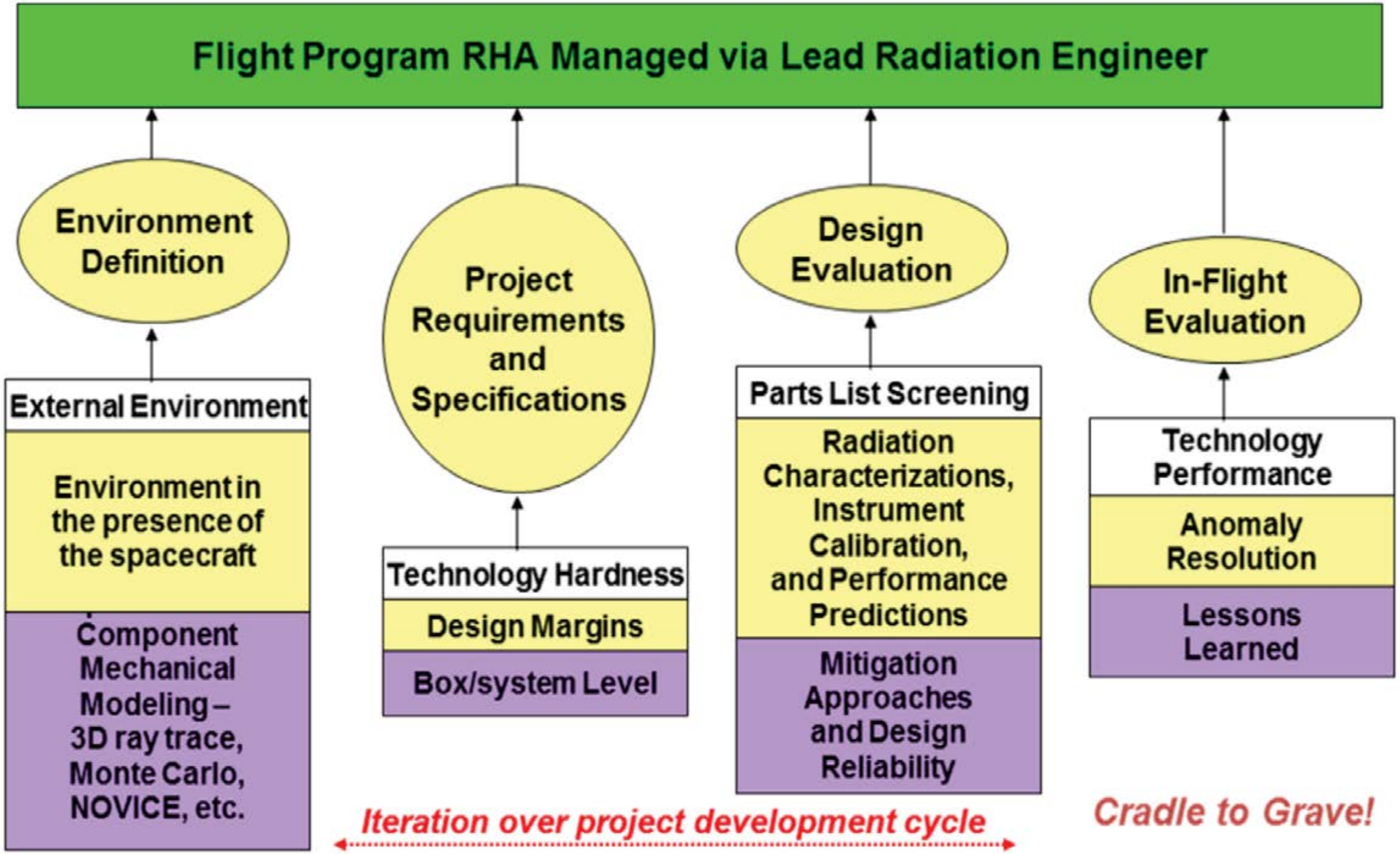
Ref - Goal:2
System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Radiation Parts Char...
GSN

Ref - Goal:3
System is tolerant to radiation faults and failures(NASA R&M mod).

Radiation Fault Tole...
GSN

Overall RHA Process



Flight Program RHA Managed via Lead Radiation Engineer

Environment Definition

External Environment

Environment in the presence of the spacecraft

Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Project Requirements and Specifications

Technology Hardness

Design Margins

Box/system Level

Design Evaluation

Parts List Screening

Radiation Characterizations, Instrument Calibration, and Performance Predictions

Mitigation Approaches and Design Reliability

In-Flight Evaluation

Technology Performance

Anomaly Resolution

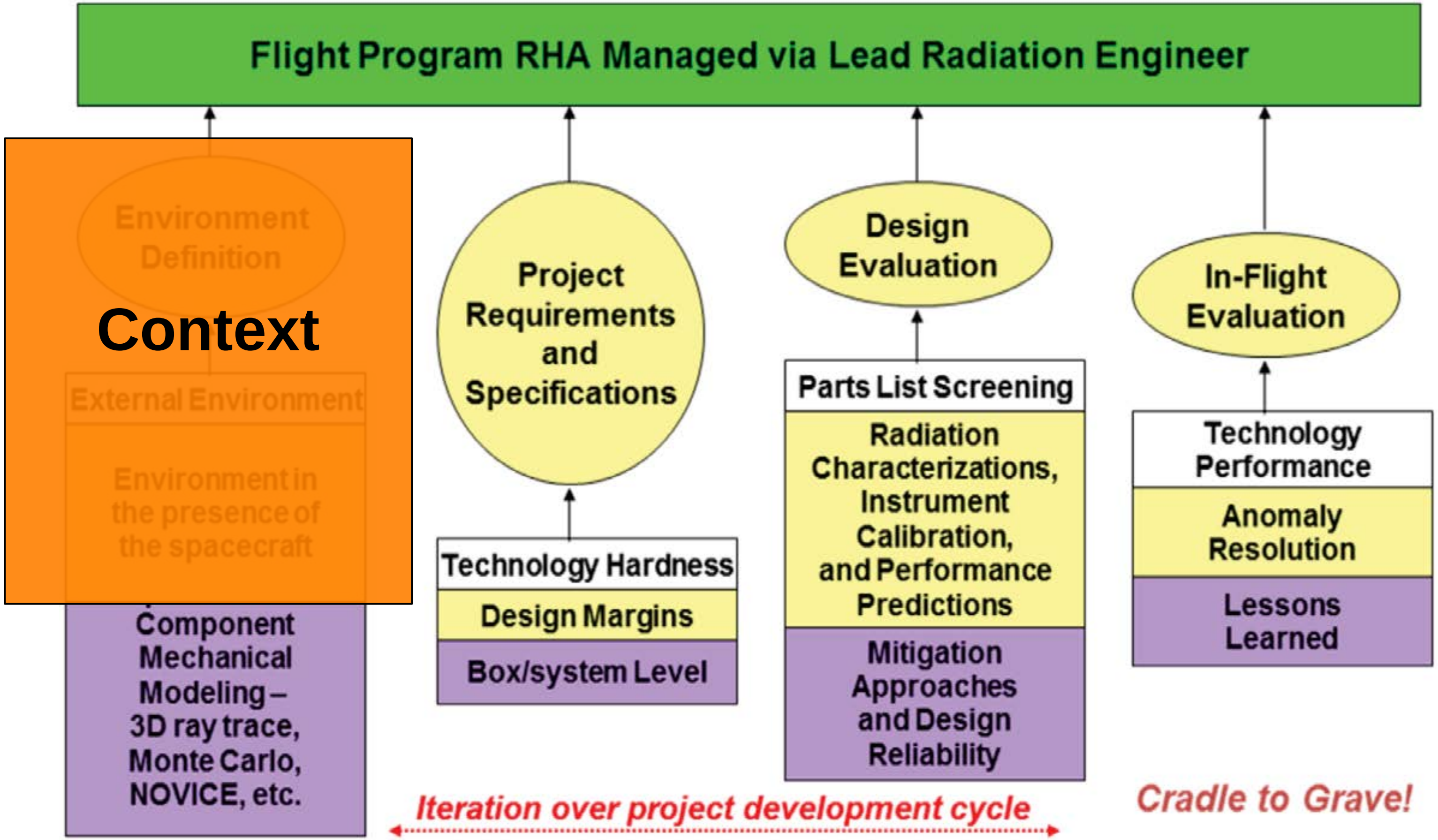
Lessons Learned

Iteration over project development cycle

Cradle to Grave!

Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014

Overall RHA Process



Flight Program RHA Managed via Lead Radiation Engineer

Environment Definition

Context

External Environment

Environment in the presence of the spacecraft

Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Project Requirements and Specifications

Technology Hardness

Design Margins

Box/system Level

Design Evaluation

Parts List Screening

Radiation Characterizations, Instrument Calibration, and Performance Predictions

Mitigation Approaches and Design Reliability

In-Flight Evaluation

Technology Performance

Anomaly Resolution

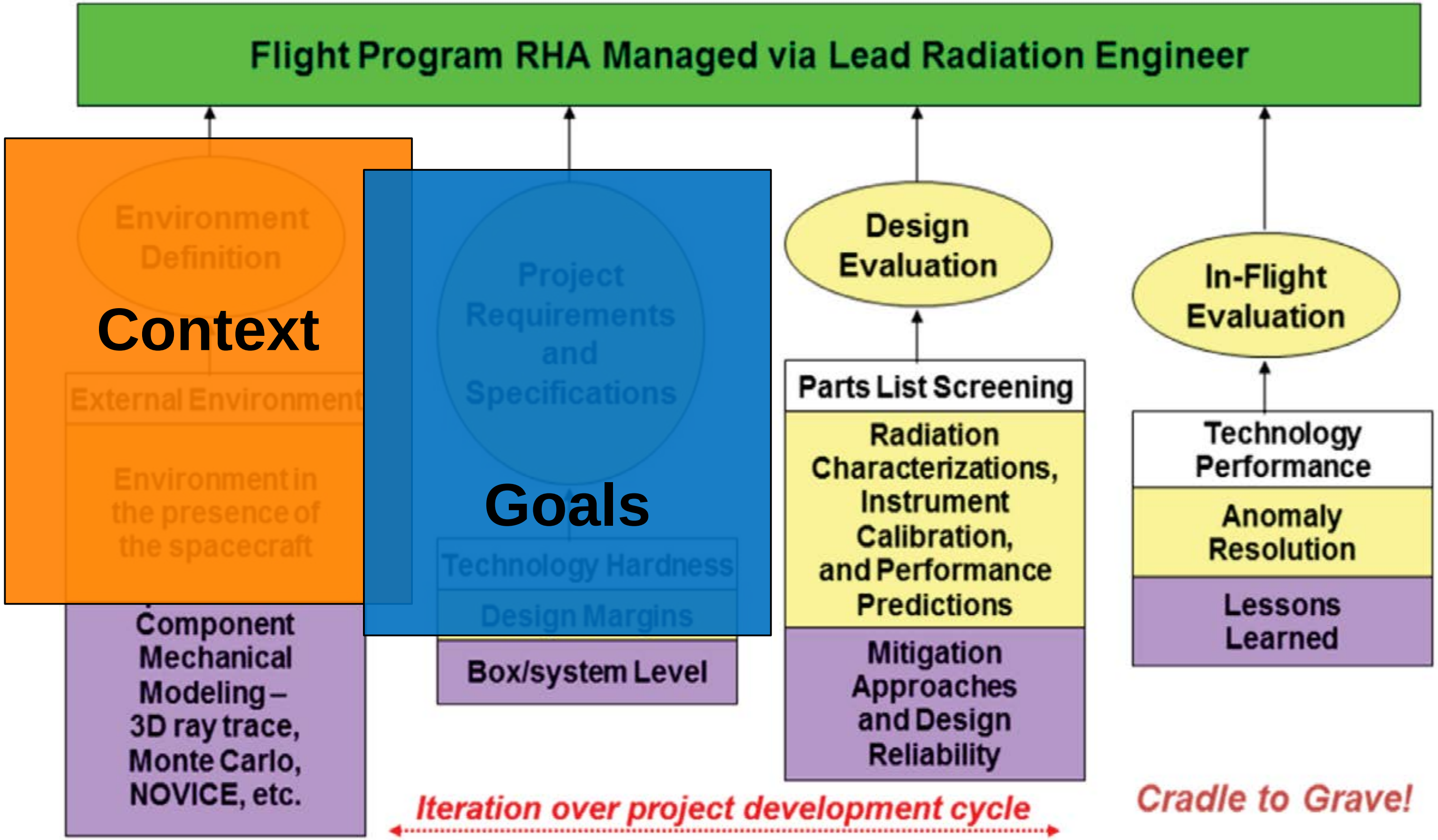
Lessons Learned

Iteration over project development cycle

Cradle to Grave!

Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014

Overall RHA Process



Flight Program RHA Managed via Lead Radiation Engineer

Environment Definition

Context

External Environment

Environment in the presence of the spacecraft

Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Project Requirements and Specifications

Goals

Technology Hardness

Design Margins

Box/system Level

Design Evaluation

Parts List Screening

Radiation Characterizations, Instrument Calibration, and Performance Predictions

Mitigation Approaches and Design Reliability

In-Flight Evaluation

Technology Performance

Anomaly Resolution

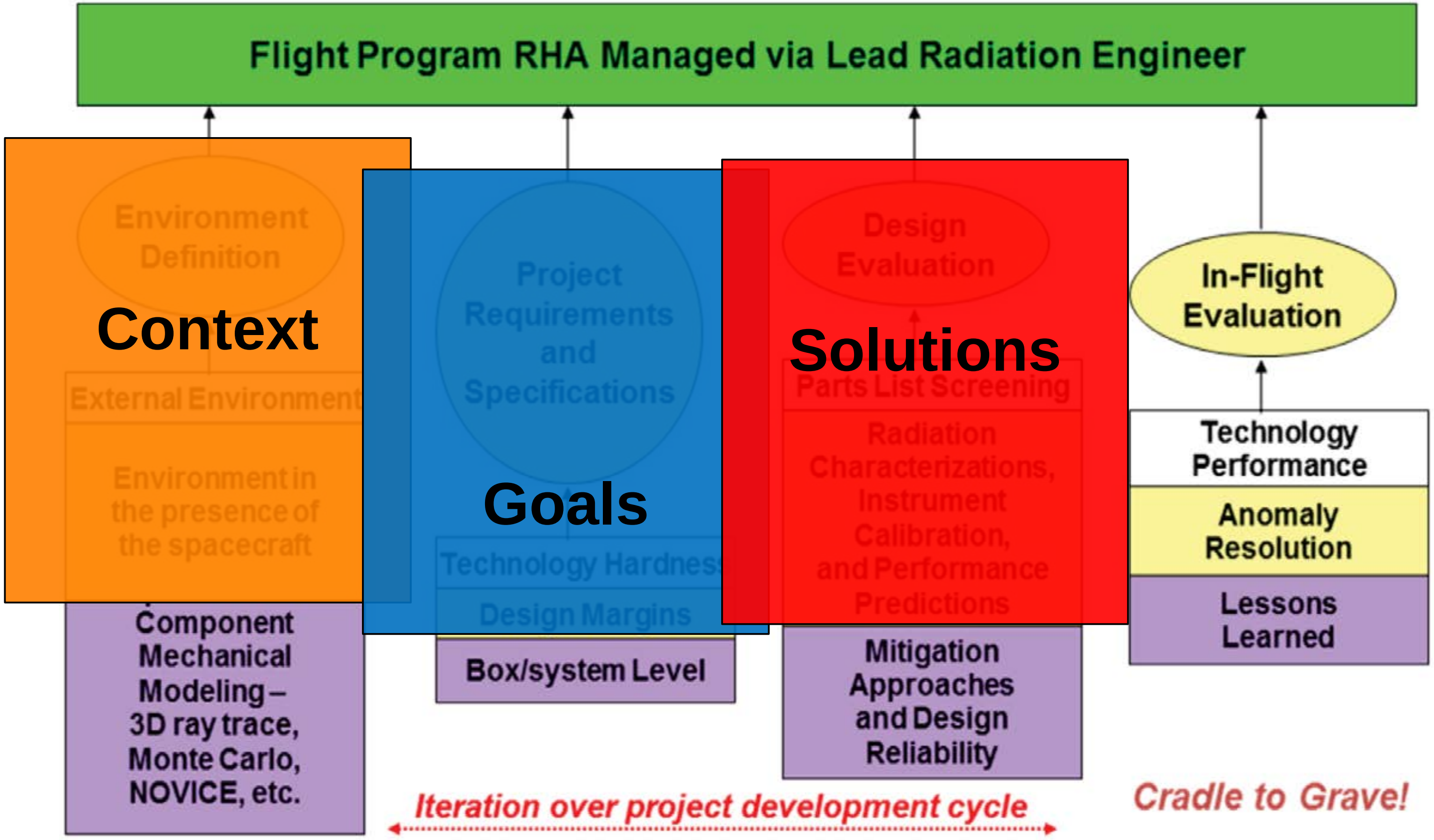
Lessons Learned

Iteration over project development cycle

Cradle to Grave!

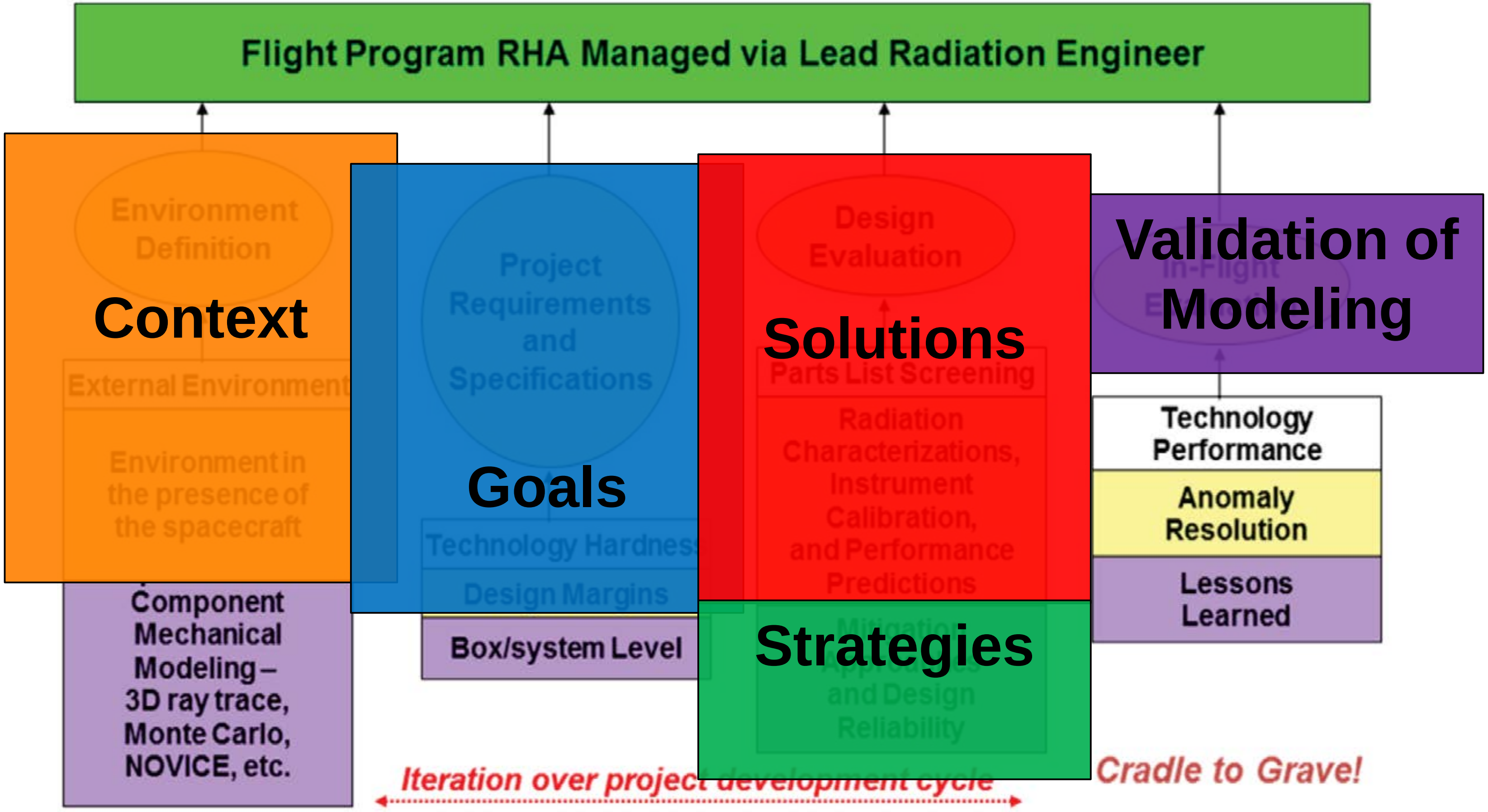
Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014

Overall RHA Process


Flight Program RHA Managed via Lead Radiation Engineer
Environment Definition
Context
External Environment
Environment in the presence of the spacecraft
Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.
Project Requirements and Specifications
Goals
Technology Hardness
Design Margins
Box/system Level
Design Evaluation
Solutions
Parts List Screening
Radiation Characterizations, Instrument Calibration, and Performance Predictions
Mitigation Approaches and Design Reliability
In-Flight Evaluation
Technology Performance
Anomaly Resolution
Lessons Learned
Iteration over project development cycle
Cradle to Grave!

Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014

Overall RHA Process

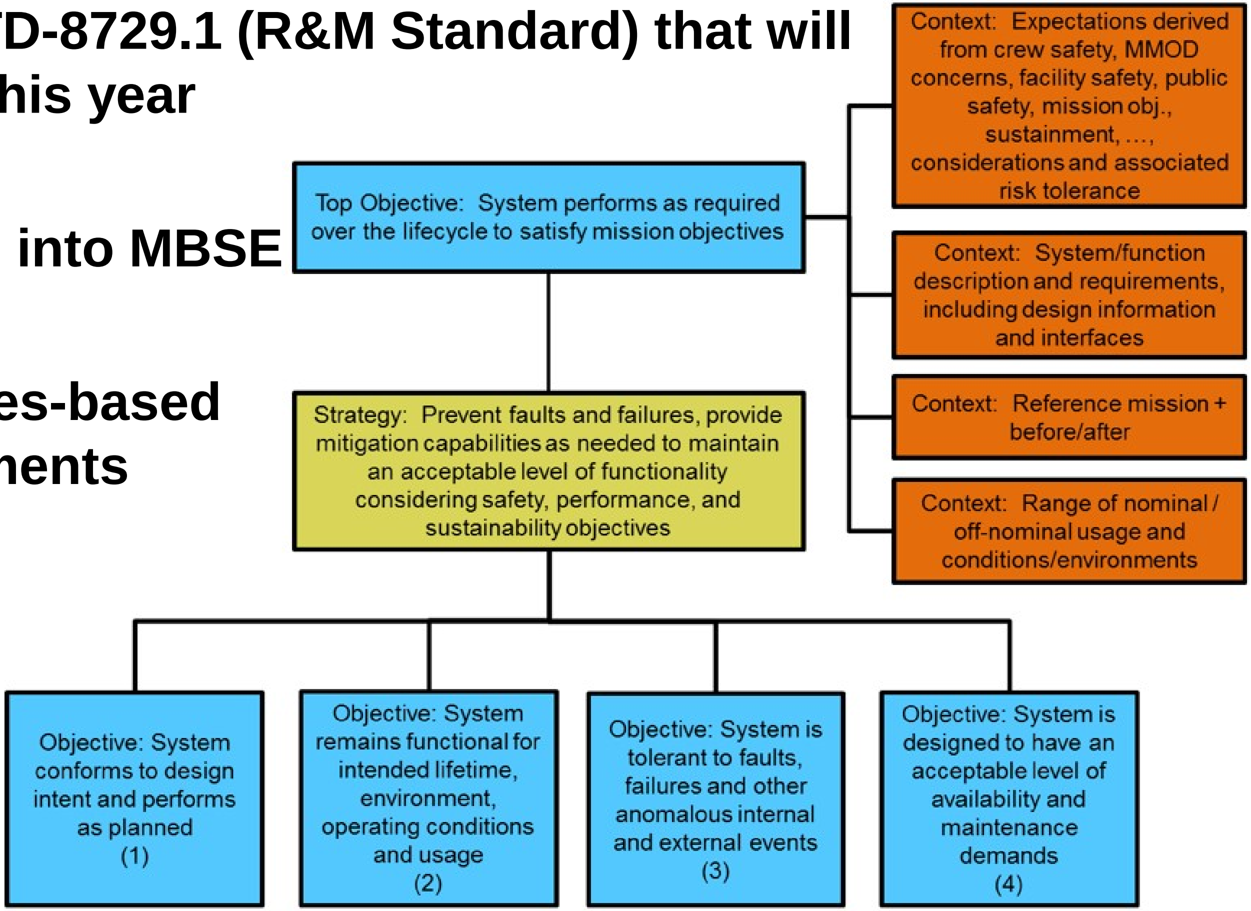

Flight Program RHA Managed via Lead Radiation Engineer
Context
Environment Definition
External Environment
Environment in the presence of the spacecraft
Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.
Goals
Project Requirements and Specifications
Technology Hardness
Design Margins
Box/system Level
Solutions
Design Evaluation
Parts List Screening
Radiation Characterizations, Instrument Calibration, and Performance Predictions
Strategies
Mitigation Approaches and Design Reliability
Validation of Modeling
In-Flight Evaluation
Technology Performance
Anomaly Resolution
Lessons Learned
Iteration over project development cycle
Cradle to Grave!

Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014

Foundation: NASA Reliability & Maintainability (R&M) Hierarchy

Vanderbilt Engineering

- Basis of NASA-STD-8729.1 (R&M Standard) that will be released later this year
- Incorporates R&M into MBSE
- Moves to objectives-based reliability requirements



Top Objective: System performs as required over the lifecycle to satisfy mission objectives

Context: Expectations derived from crew safety, MMOD concerns, facility safety, public safety, mission obj., sustainment, …, considerations and associated risk tolerance

Context: System/function description and requirements, including design information and interfaces

Context: Reference mission + before/after

Context: Range of nominal / off-nominal usage and conditions/environments

Strategy: Prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives

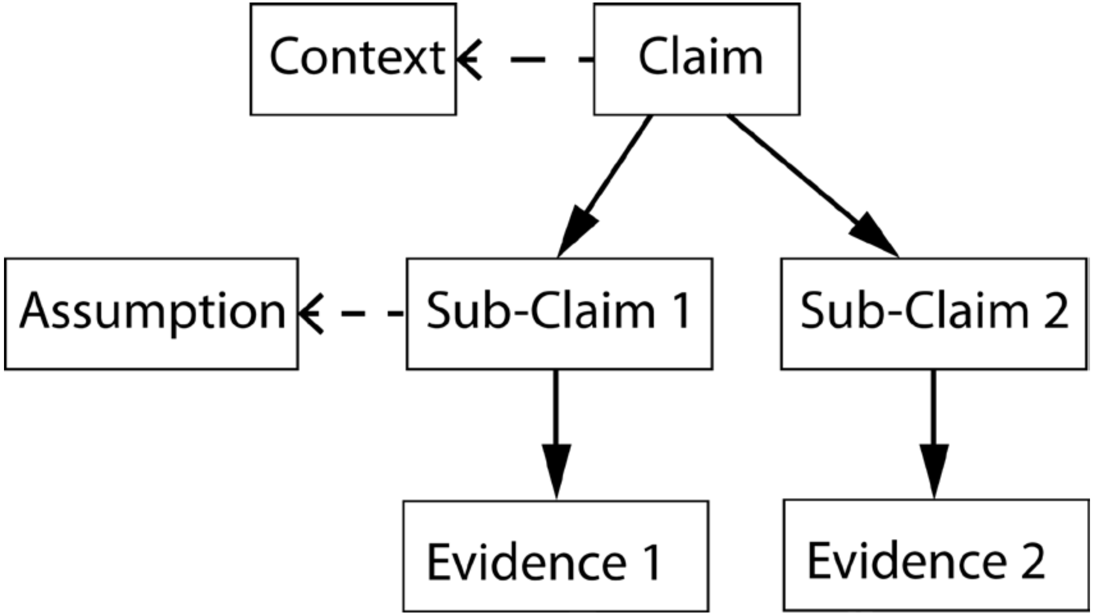
Objective: System conforms to design intent and performs as planned (1)

Objective: System remains functional for intended lifetime, environment, operating conditions and usage (2)

Objective: System is tolerant to faults, failures and other anomalous internal and external events (3)

Objective: System is designed to have an acceptable level of availability and maintenance demands (4)

Graphical Assurance Cases



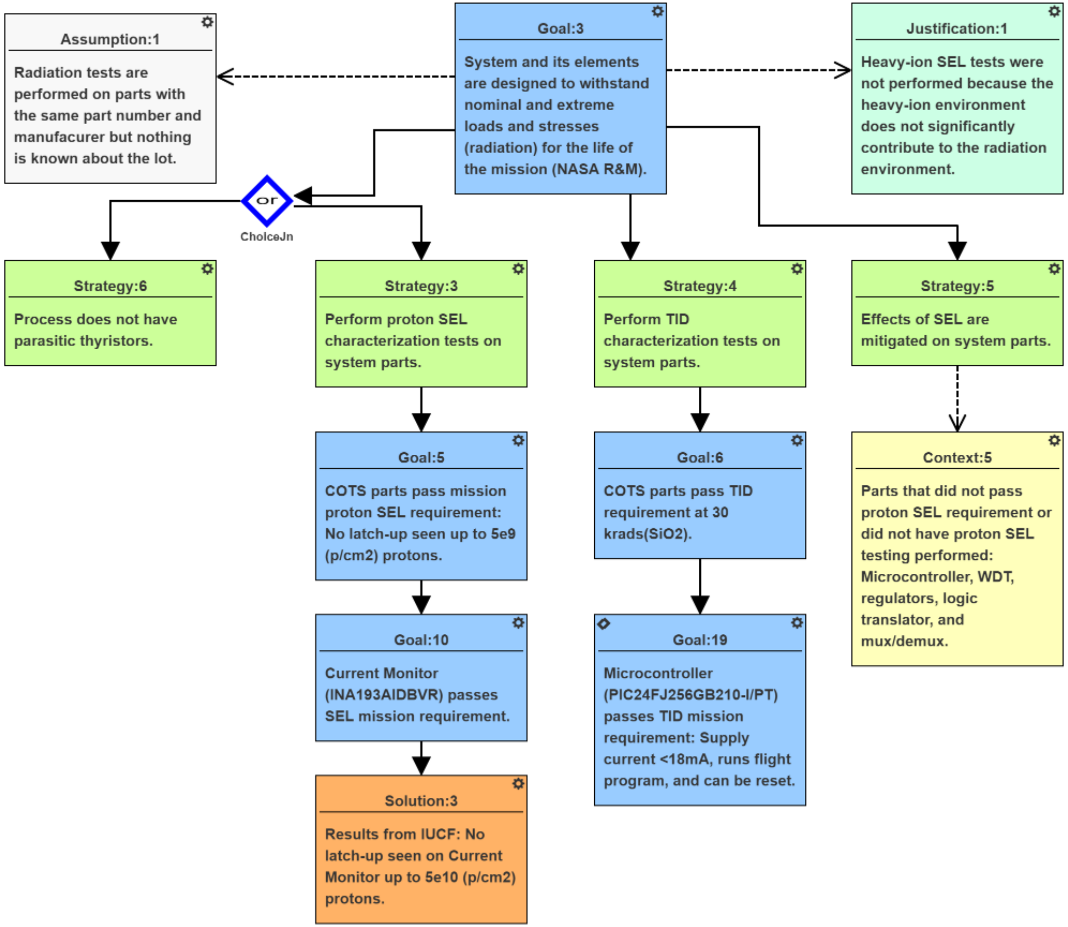
Argument: “A connected series of claims intended to support an overall claim.” [1]

Assurance Case: “A reasoned and compelling argument, supported by a body of evidence, that a system, service or organization will operate as intended for a defined application in a defined environment.” [1]

[1] GSN Community Standard Version 1 2011

Goal Structuring Notation (GSN): Visual Representation of an Argument

Vanderbilt Engineering



Assumption:1

Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:3

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1

Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6

Process does not have parasitic thyristors.

Strategy:3

Perform proton SEL characterization tests on system parts.

Strategy:4

Perform TID characterization tests on system parts.

Strategy:5

Effects of SEL are mitigated on system parts.

Goal:5

COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6

COTS parts pass TID requirement at 30 krads(SiO2).

Context:5

Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10

Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19

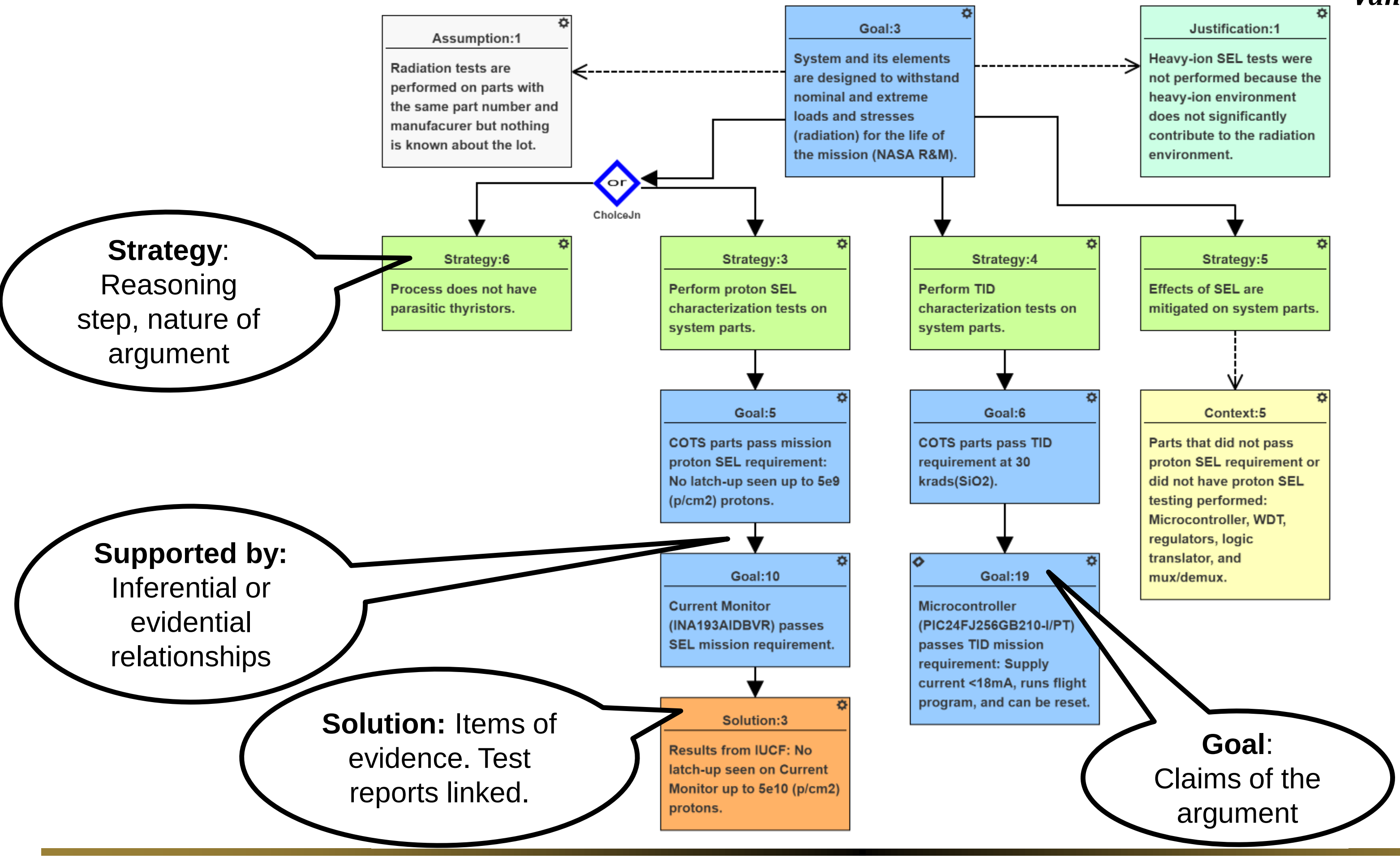
Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3

Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

Goal Structuring Notation (GSN): Visual Representation of an Argument

Vanderbilt Engineering



Goal:3

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Assumption:1

Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Justification:1

Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6

Process does not have parasitic thyristors.

Strategy:3

Perform proton SEL characterization tests on system parts.

Strategy:4

Perform TID characterization tests on system parts.

Strategy:5

Effects of SEL are mitigated on system parts.

Goal:5

COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6

COTS parts pass TID requirement at 30 krads(SiO2).

Context:5

Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10

Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19

Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3

Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

Strategy: Reasoning step, nature of argument

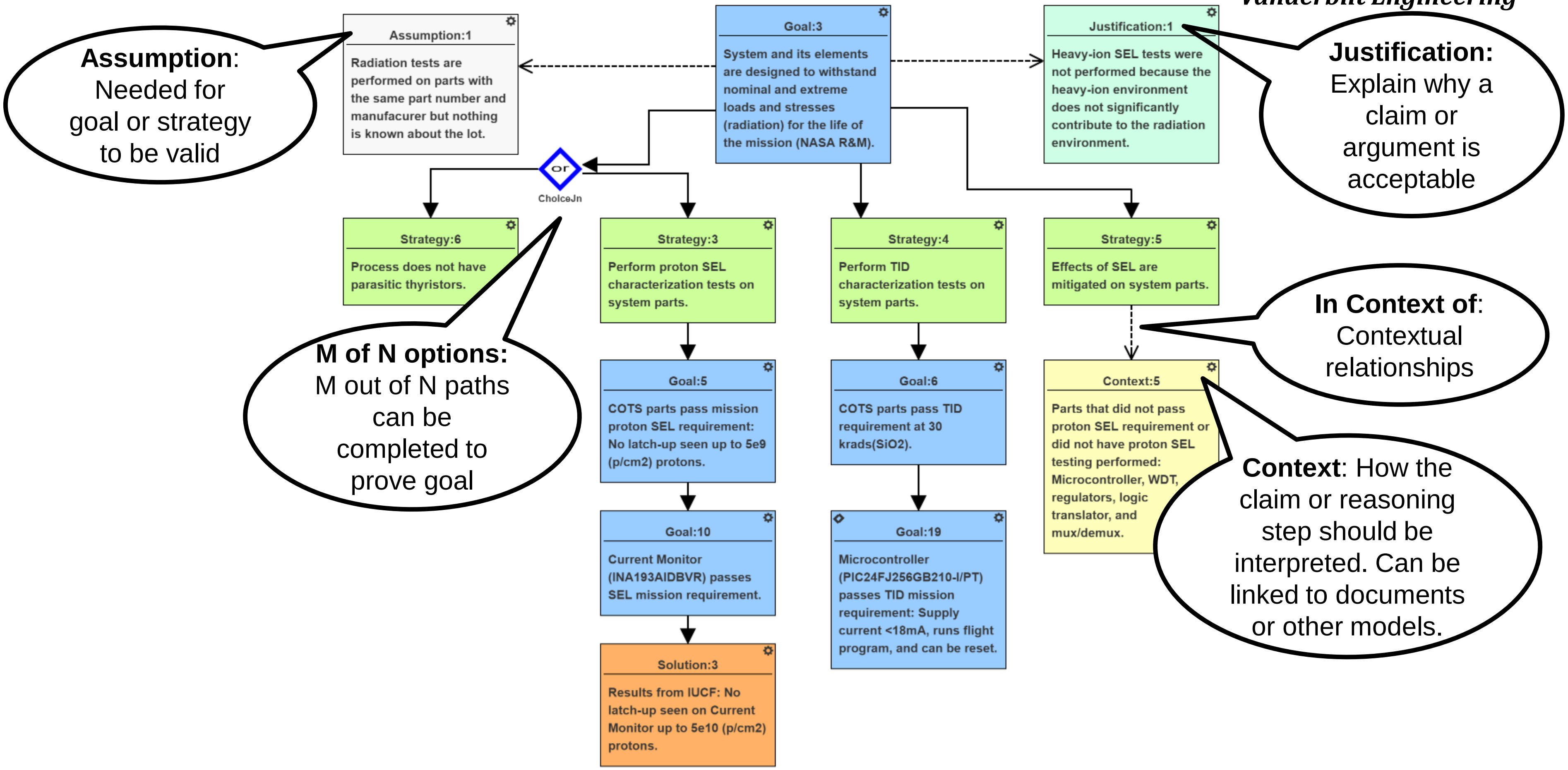
Supported by: Inferential or evidential relationships

Solution: Items of evidence. Test reports linked.

Goal: Claims of the argument

Goal Structuring Notation (GSN): Visual Representation of an Argument

Vanderbilt Engineering



Assumption: Needed for goal or strategy to be valid

Assumption:1

Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:3

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1

Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Justification: Explain why a claim or argument is acceptable

Strategy:6

Process does not have parasitic thyristors.

Strategy:3

Perform proton SEL characterization tests on system parts.

Strategy:4

Perform TID characterization tests on system parts.

Strategy:5

Effects of SEL are mitigated on system parts.

In Context of: Contextual relationships

M of N options: M out of N paths can be completed to prove goal

Goal:5

COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6

COTS parts pass TID requirement at 30 krads(SiO2).

Context:5

Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Context: How the claim or reasoning step should be interpreted. Can be linked to documents or other models.

Goal:10

Current Monitor (INA193AIDBVR) passes SEL mission requirement.

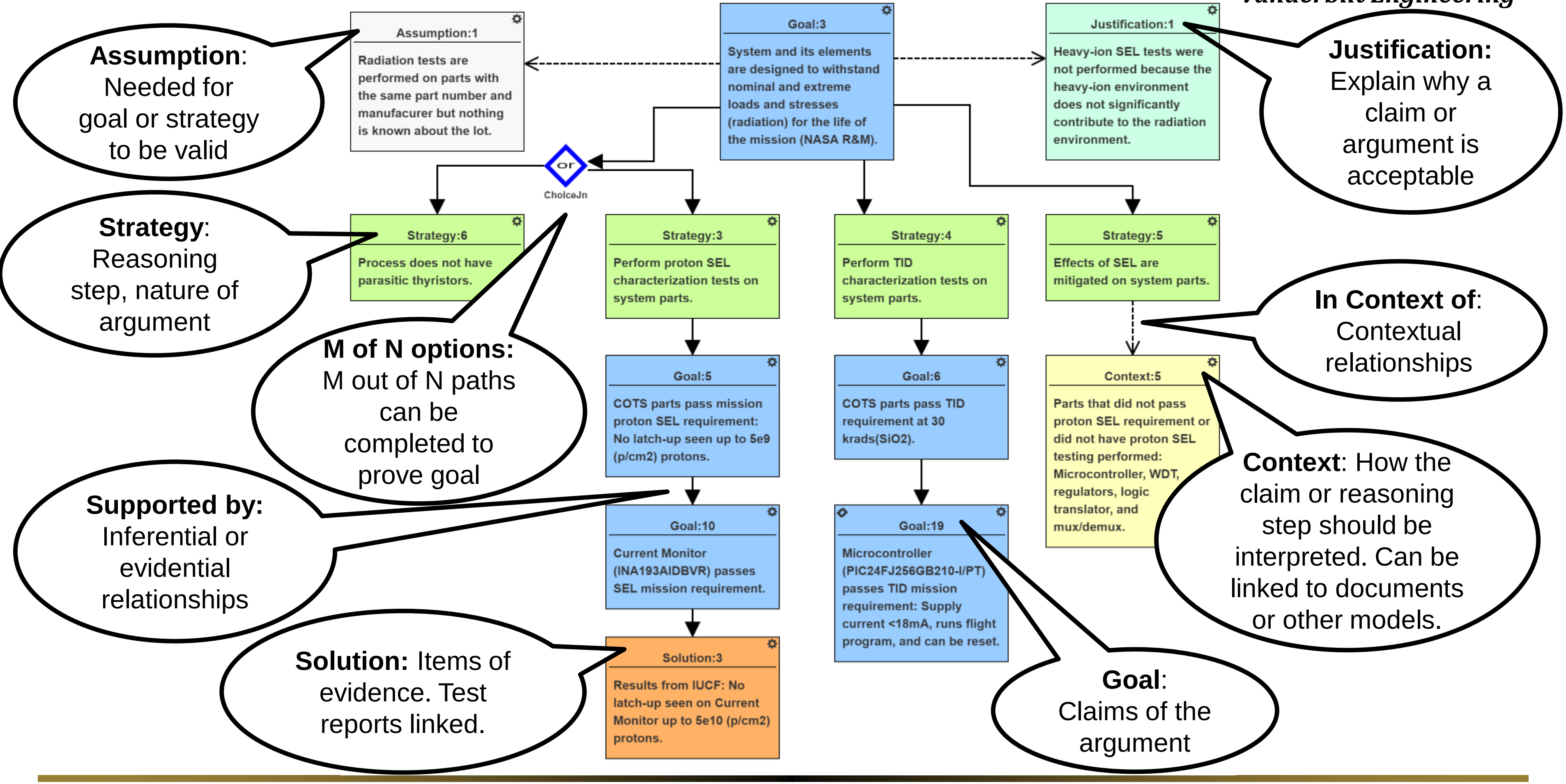
Goal:19

Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3

Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

Goal Structuring Notation (GSN): Visual Representation of an Argument



Assumption:1

Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:3

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1

Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6

Process does not have parasitic thyristors.

Strategy:3

Perform proton SEL characterization tests on system parts.

Strategy:4

Perform TID characterization tests on system parts.

Strategy:5

Effects of SEL are mitigated on system parts.

Goal:5

COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6

COTS parts pass TID requirement at 30 krads(SiO2).

Context:5

Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10

Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19

Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3

Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

Assumption: Needed for goal or strategy to be valid

Justification: Explain why a claim or argument is acceptable

Strategy: Reasoning step, nature of argument

In Context of: Contextual relationships

M of N options: M out of N paths can be completed to prove goal

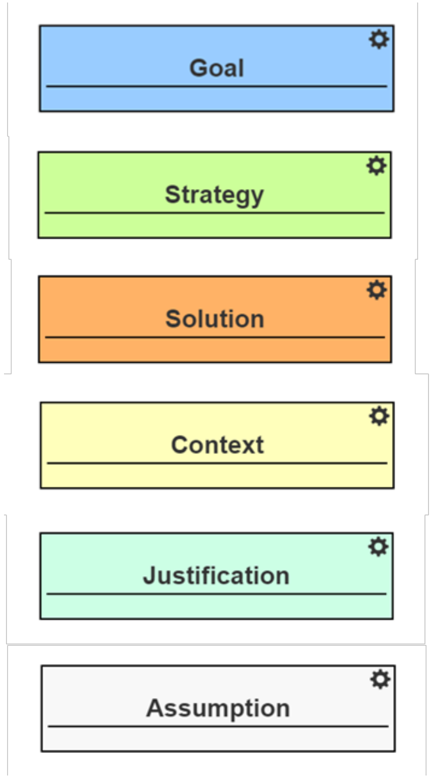
Context: How the claim or reasoning step should be interpreted. Can be linked to documents or other models.

Supported by: Inferential or evidential relationships

Solution: Items of evidence. Test reports linked.

Goal: Claims of the argument

Goal Structuring Notation (GSN): Visual Representation of an Argument



Goal: Claims of the argument

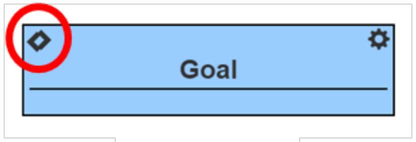
Strategy: Reasoning step, nature of argument

Solution: Items of evidence

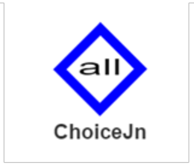
Context: How the claim or reasoning step should be interpreted

Justification: Explains why a claim or argument is acceptable

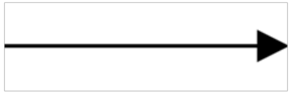
Assumption: Needed for goal or strategy to be valid



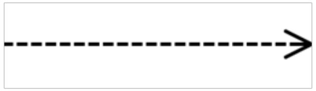
Undeveloped entity symbol: Indicates the line of reasoning is not complete



M of N options: M out of N paths can be complete to prove goal



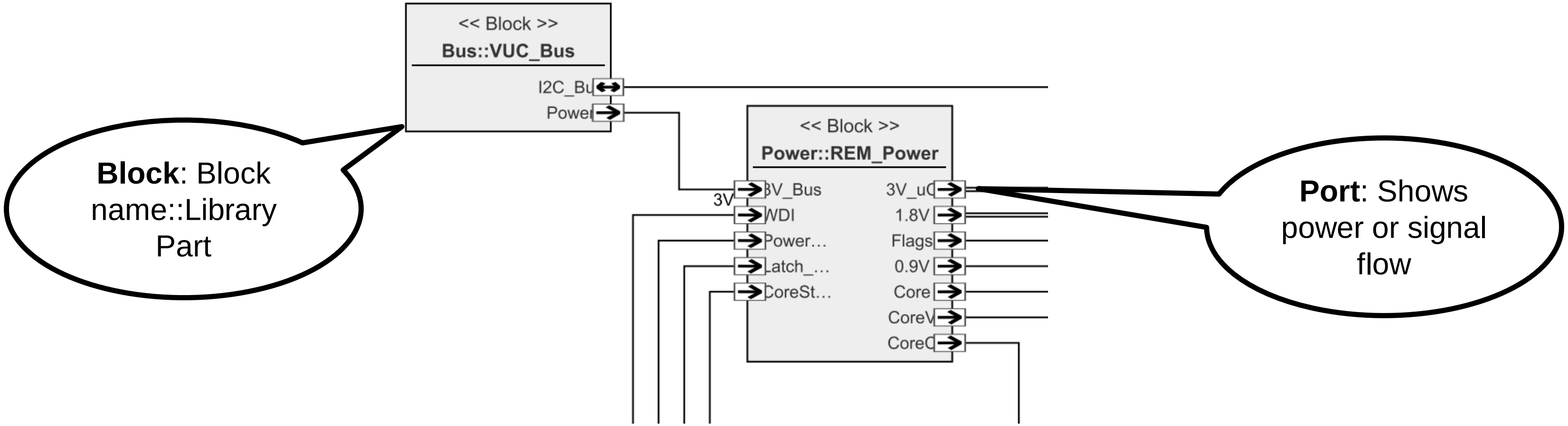
Supported by: Inferential or evidential relationships



In context of: Contextual relationships

System Modeling Language (SysML)

- **Graphical modeling language that supports specification, analysis, design, verification, and validation of systems**
  - Systems include hardware, software, data, personnel, procedures, and facilities
- **MBAC+ just uses the Block Diagram modeling standard from SysML at the moment**



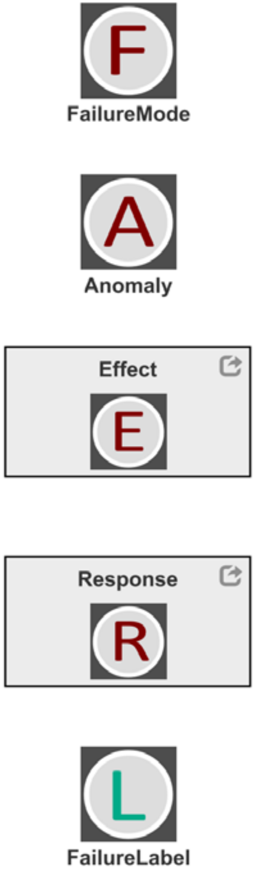
Block: Block name::Library Part

Port: Shows power or signal flow

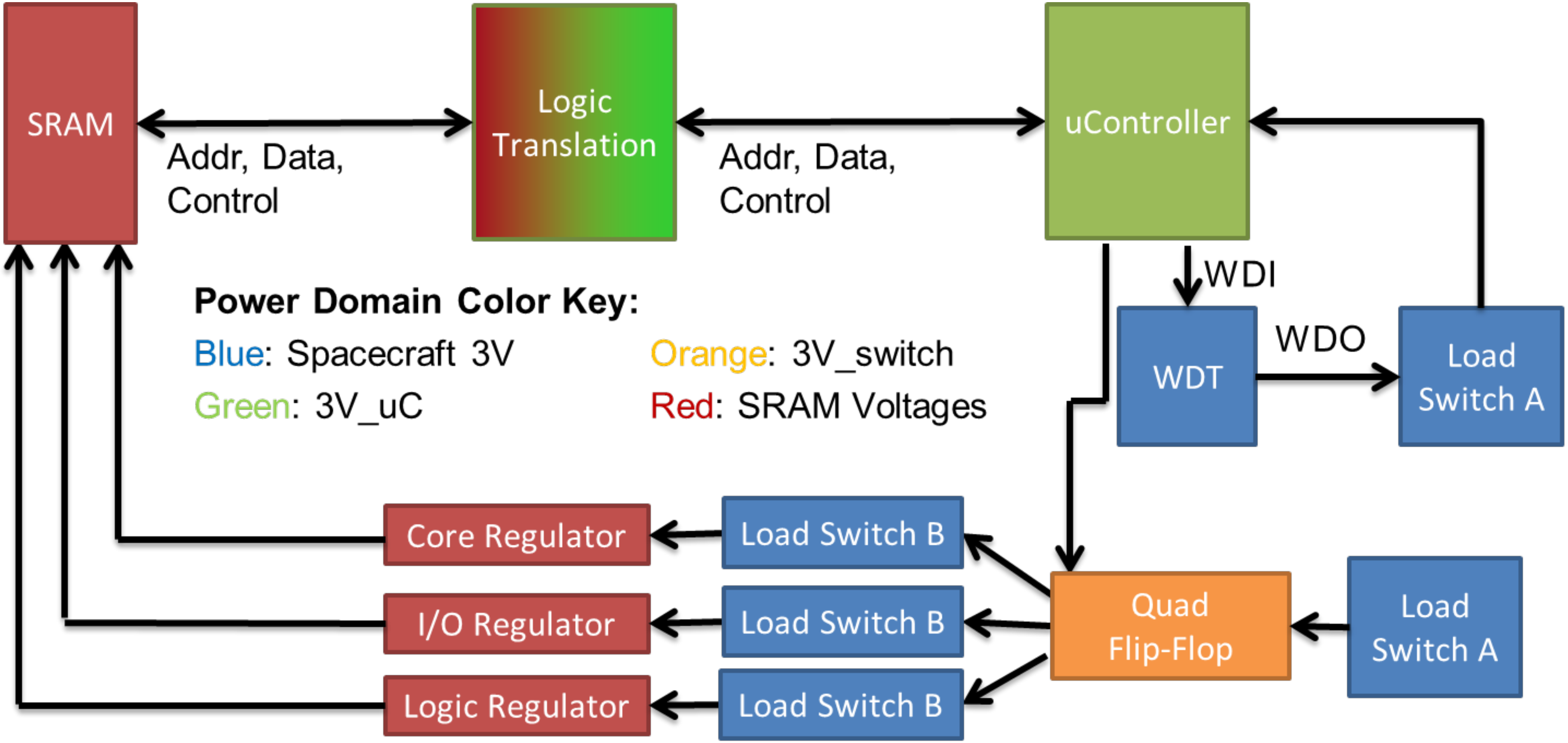
Radiation Fault Propagation Modeling

- **Fault (F): Change in physical operation, depart from nominal**
- **Anomaly (A): Observable effect or anomalous behavior from fault**
- **Response (R): Intended response of component to A and F (mitigation)**
- **Effects (E): Impact on functionality**

- **Faults/Anomalies flow through ports to affect other components**



CubeSat SRAM Experiment Board



Power Domain Color Key:

Blue: Spacecraft 3V

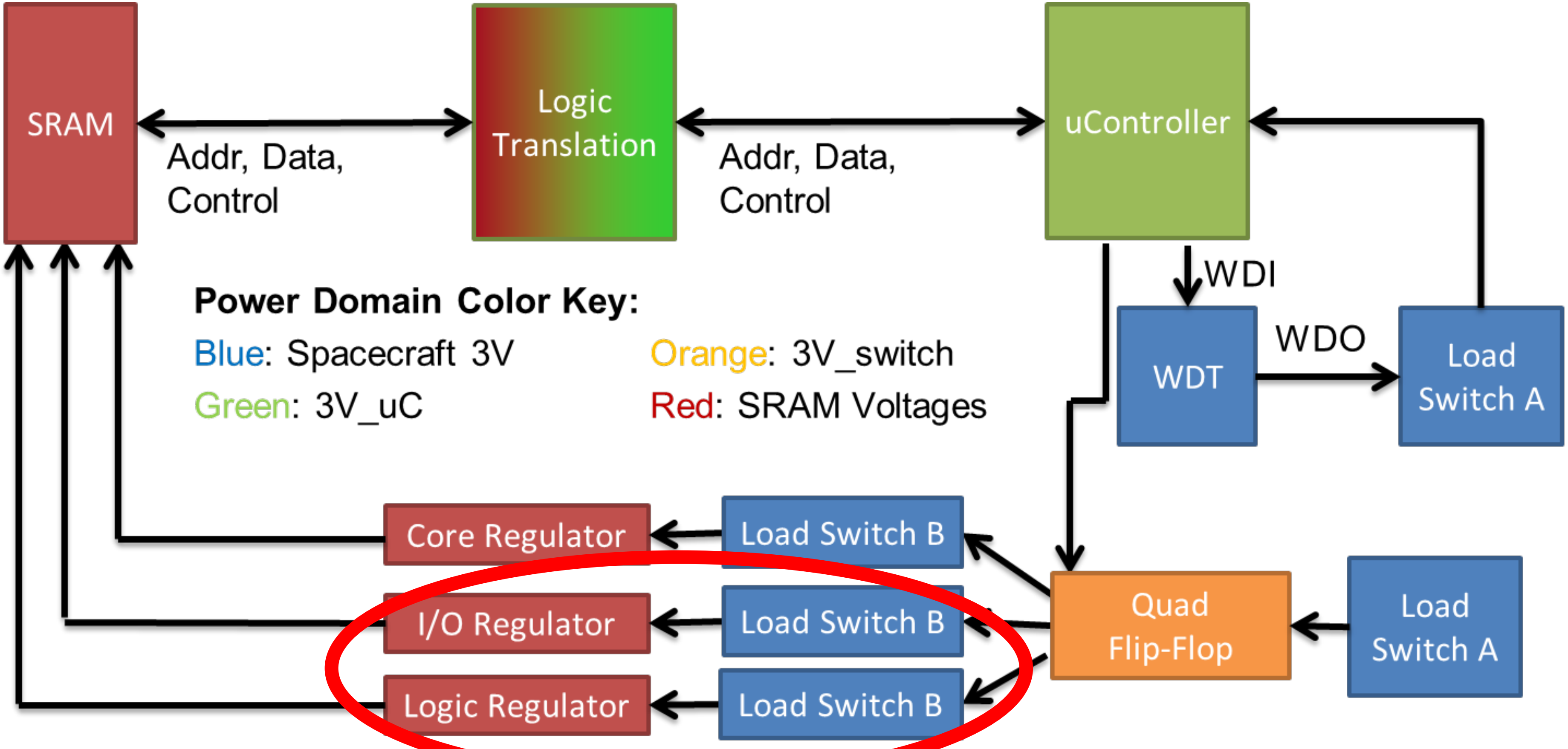
Green: 3V_uC

Orange: 3V_switch

Red: SRAM Voltages

CubeSat SRAM Experiment Board

Vanderbilt Engineering



Power Domain Color Key:

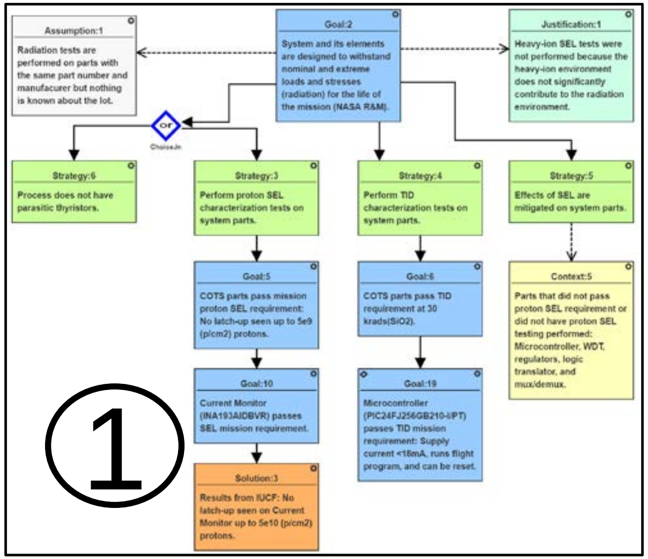
Blue: Spacecraft 3V

Green: 3V_uC

Orange: 3V_switch

Red: SRAM Voltages

MBAC+ Modeling Flow



Goal:2

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Assumption:1

Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Justification:1

Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6

Process does not have parasitic thyristors.

Strategy:3

Perform proton SEL characterization tests on system parts.

Strategy:4

Perform TID characterization tests on system parts.

Strategy:5

Effects of SEL are mitigated on system parts.

Goal:5

COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6

COTS parts pass TID requirement at 30 krads(SiO2).

Context:5

Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10

Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19

Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

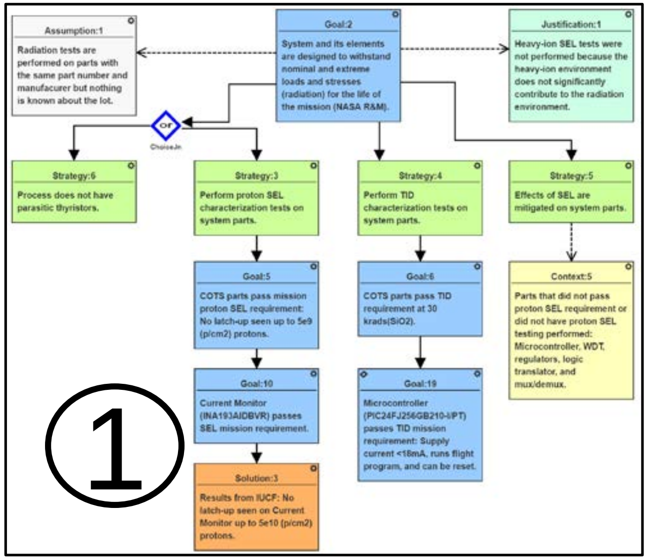
Solution:3

Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

1) Determine mission objective and fill in top-level of R&M Template

MBAC+ Modeling Flow

Vanderbilt Engineering



Assumption:1
Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:2
System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1
Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6
Process does not have parasitic thyristors.

Strategy:3
Perform proton SEL characterization tests on system parts.

Strategy:4
Perform TID characterization tests on system parts.

Strategy:5
Effects of SEL are mitigated on system parts.

Goal:5
COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6
COTS parts pass TID requirement at 30 krads(SiO2).

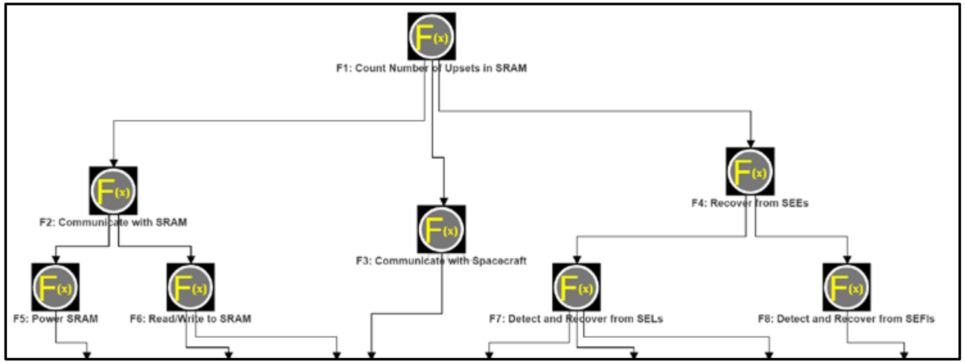
Context:5
Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10
Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19
Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

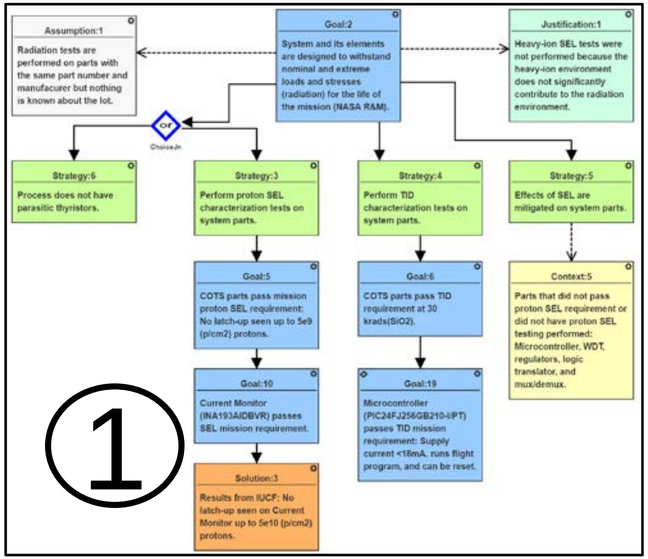
Solution:3
Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

②


F1: Count Number of Upsets in SRAM
F2: Communicate with SRAM
F3: Communicate with Spacecraft
F4: Recover from SEEs
F5: Power SRAM
F6: Read/Write to SRAM
F7: Detect and Recover from SELs
F8: Detect and Recover from SEFIs

2) Create functional decomposition of system

MBAC+ Modeling Flow



Assumption:1
Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:2
System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1
Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6
Process does not have parasitic thyristors.

Strategy:3
Perform proton SEL characterization tests on system parts.

Strategy:4
Perform TID characterization tests on system parts.

Strategy:5
Effects of SEL are mitigated on system parts.

Goal:5
COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6
COTS parts pass TID requirement at 30 krads(SiO2).

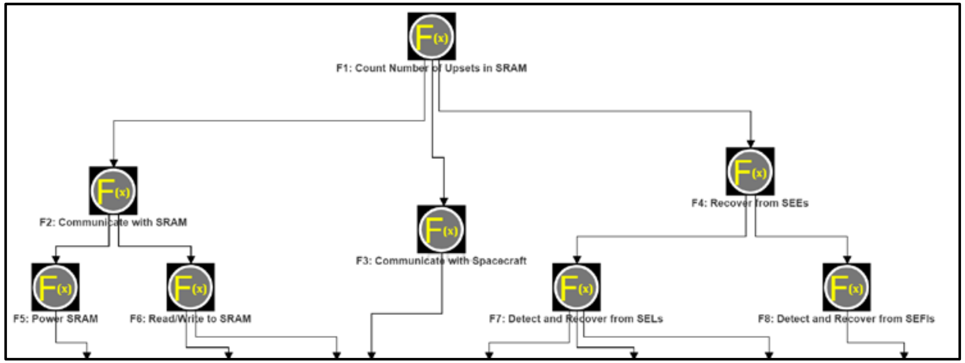
Context:5
Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10
Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19
Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

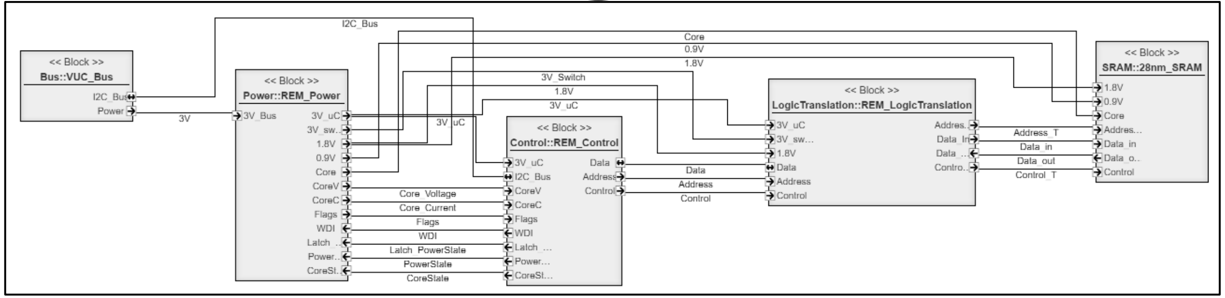
Solution:3
Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

2

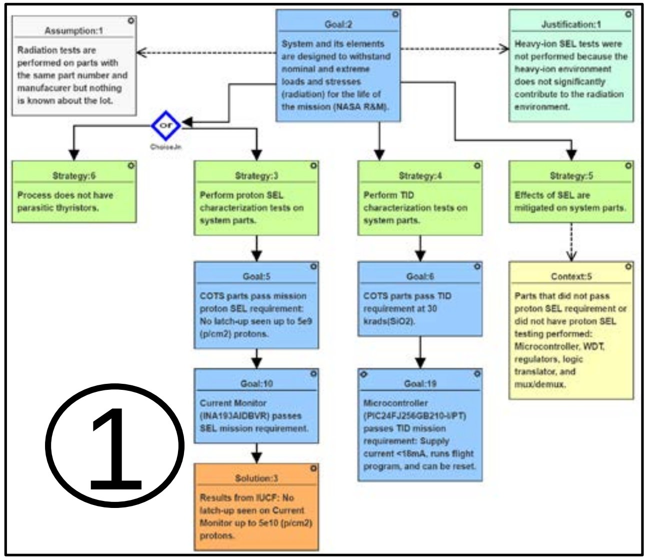

F(x)
F1: Count Number of Upsets in SRAM
F2: Communicate with SRAM
F3: Communicate with Spacecraft
F4: Recover from SEEs
F5: Power SRAM
F6: Read/Write to SRAM
F7: Detect and Recover from SELs
F8: Detect and Recover from SEFIs

3) Create SysML Block Diagram

3



MBAC+ Modeling Flow



Assumption:1
Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:2
System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1
Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6
Process does not have parasitic thyristors.

Strategy:3
Perform proton SEL characterization tests on system parts.

Strategy:4
Perform TID characterization tests on system parts.

Strategy:5
Effects of SEL are mitigated on system parts.

Goal:5
COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

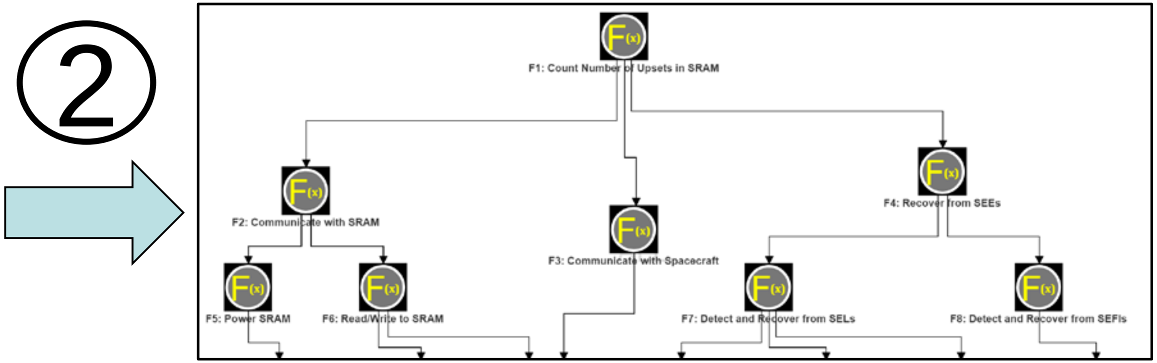
Goal:6
COTS parts pass TID requirement at 30 krads(SiO2).

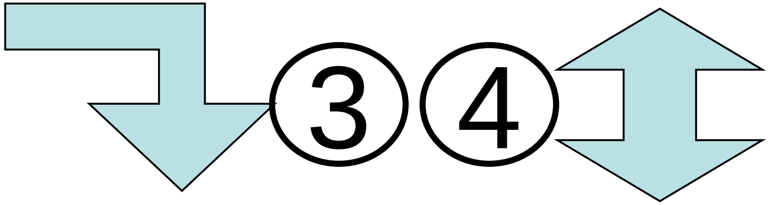
Context:5
Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10
Current Monitor (INA193AIDBVR) passes SEL mission requirement.

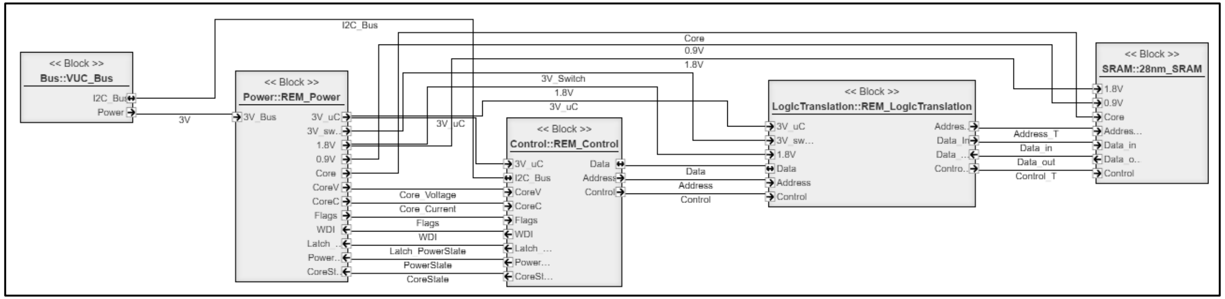
Goal:19
Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3
Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

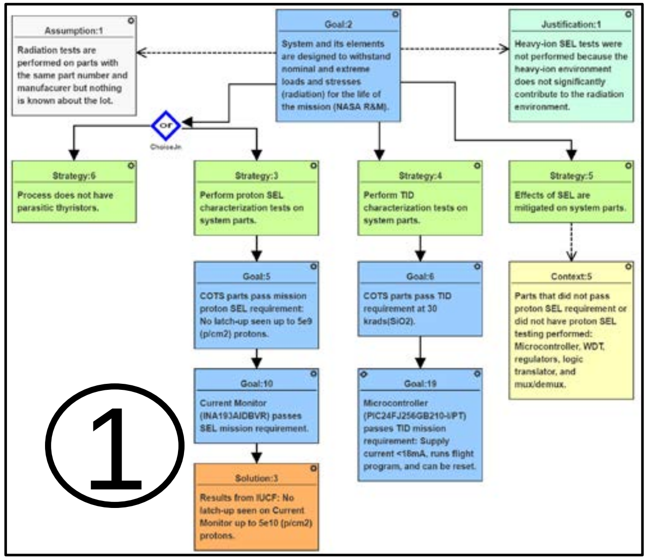

②
F(x)
F1: Count Number of Upsets in SRAM
F2: Communicate with SRAM
F3: Communicate with Spacecraft
F4: Recover from SEEs
F5: Power SRAM
F6: Read/Write to SRAM
F7: Detect and Recover from SELs
F8: Detect and Recover from SEFIs



4) Link functions with block diagram



MBAC+ Modeling Flow



Assumption:1

Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:2

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1

Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6

Process does not have parasitic thyristors.

Strategy:3

Perform proton SEL characterization tests on system parts.

Strategy:4

Perform TID characterization tests on system parts.

Strategy:5

Effects of SEL are mitigated on system parts.

Goal:5

COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6

COTS parts pass TID requirement at 30 krads(SiO2).

Context:5

Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10

Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19

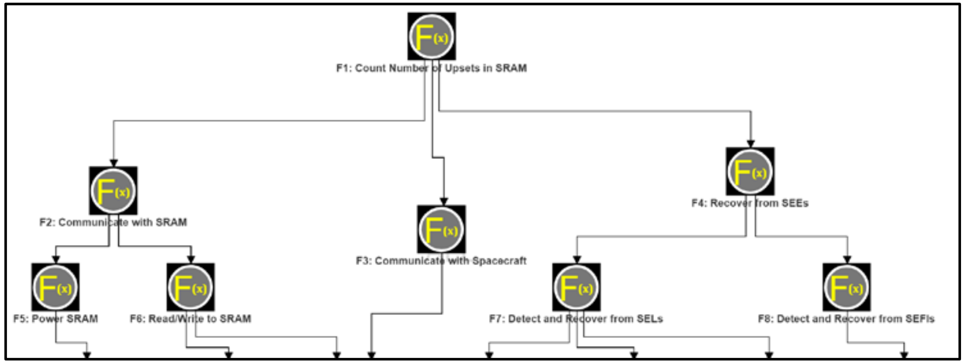
Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3

Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

①

②

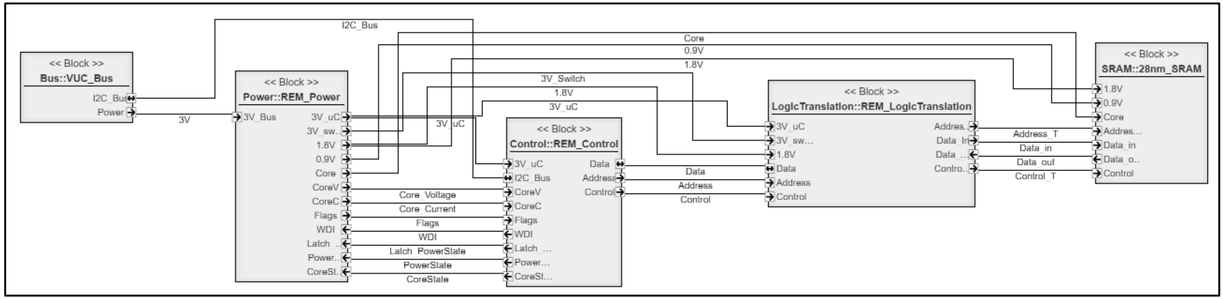


F(x)
F1: Count Number of Upsets in SRAM
F2: Communicate with SRAM
F3: Communicate with Spacecraft
F4: Recover from SEEs
F5: Power SRAM
F6: Read/Write to SRAM
F7: Detect and Recover from SELs
F8: Detect and Recover from SEFIs

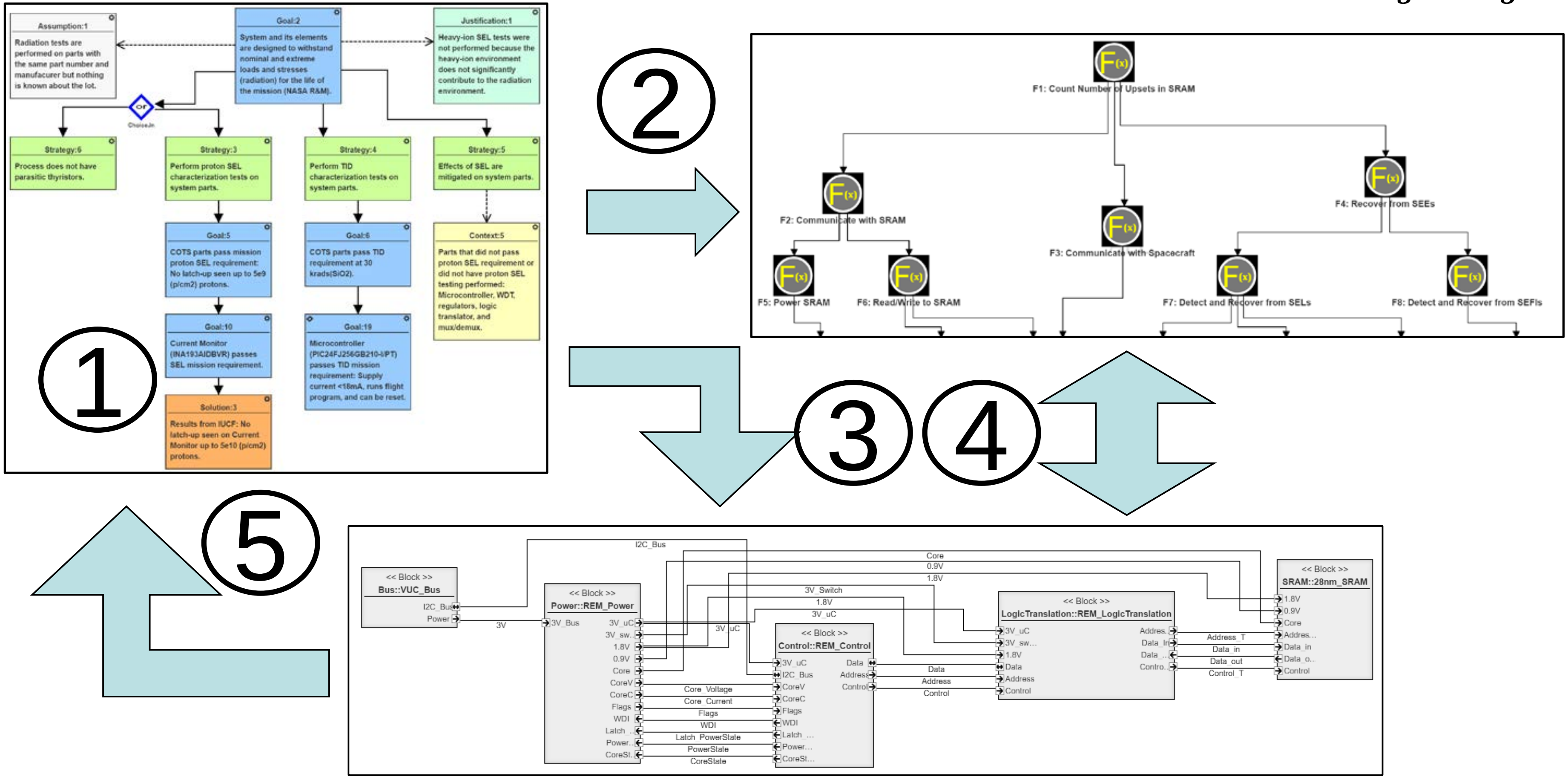
③ ④

5) Complete assurance case based on system design and test results

⑤



MBAC+ Modeling Flow



Assumption:1
Radiation tests are performed on parts with the same part number and manufacurer but nothing is known about the lot.

Goal:2
System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Justification:1
Heavy-ion SEL tests were not performed because the heavy-ion environment does not significantly contribute to the radiation environment.

Strategy:6
Process does not have parasitic thyristors.

Strategy:3
Perform proton SEL characterization tests on system parts.

Strategy:4
Perform TID characterization tests on system parts.

Strategy:5
Effects of SEL are mitigated on system parts.

Goal:5
COTS parts pass mission proton SEL requirement: No latch-up seen up to 5e9 (p/cm2) protons.

Goal:6
COTS parts pass TID requirement at 30 krads(SiO2).

Context:5
Parts that did not pass proton SEL requirement or did not have proton SEL testing performed: Microcontroller, WDT, regulators, logic translator, and mux/demux.

Goal:10
Current Monitor (INA193AIDBVR) passes SEL mission requirement.

Goal:19
Microcontroller (PIC24FJ256GB210-I/PT) passes TID mission requirement: Supply current <18mA, runs flight program, and can be reset.

Solution:3
Results from IUCF: No latch-up seen on Current Monitor up to 5e10 (p/cm2) protons.

Live Demo

https://modelbasedassurance.org/

1) R&M Hierarchy as seed model
2) Use R&M Hierarchy as a template for example radiation reliability assurance case
3) Link SysML blocks to assurance case
4) Show team assignment and group working capabilities

Site Infrastructure

- The contents of the modelbasedassurance.org website have been prepared for the Radiation Effects research community for informational purposes that are not export controlled. Your privacy and security are important to us; please do not upload any data that is controlled unclassified information, export controlled, or considered to be intellectual property.

- You can make your own site (internal server, amazon gov cloud, etc.) if you want to include Export/ITAR material. Contact us.